

**DISEÑO DEL ANALISIS DE RIESGO DEL PROCESO TECNOLOGICO DE LA CAJA DE
COMPENSACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA”, PARA LA APLICACIÓN
DEL SISTEMA DE CONTROL INTERNO SUBSIDIO FAMILIAR SCISF, SEGÚN CIRCULAR
0023 DEL 30 DE NOVIEMBRE DE 2010, DE LA SUPERINTENDENCIA DE SUBSIDIO
FAMILIAR**

**ROSA ESTUPIÑAN MEJIA
MIRLEDIS MARTINEZ LEAL**

**CORPORACION UNIVERSITARIA DE LA COSTA
FACULTAD DE CONTADURIA
ESPECIALIZACION EN AUDITORIA DE SISTEMAS DE INFORMACION
BARRANQUILLA - ATLANTICO
2012**

**DISEÑO DEL ANALISIS DE RIESGO DEL PROCESO TECNOLÓGICO DE LA CAJA DE
COMPENSACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA”, PARA LA APLICACIÓN
DEL SISTEMA DE CONTROL INTERNO SUBSIDIO FAMILIAR SCISF, SEGÚN CIRCULAR
0023 DEL 30 DE NOVIEMBRE DE 2010, DE LA SUPERINTENDENCIA DE SUBSIDIO
FAMILIAR**

**ROSA ESTUPIÑAN MEJIA
MIRLEDIS MARTINEZ LEAL**

**Trabajo de Grado Para Optar el Título De
Especialista en Auditoria de Sistemas de Información**

**DIRECTOR
VICTOR MONTAÑO ARDILA**

**CORPORACION UNIVERSITARIA DE LA COSTA
FACULTAD DE CONTADURIA
ESPECIALIZACION EN AUDITORIA DE SISTEMAS DE INFORMACION
BARRANQUILLA - ATLANTICO
2012**

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

DEDICATORIA

“Hijo mio, si hace tuyas mis palabras y atesoras mis mandamientos; si tu oído inclinas hacia la sabiduría y de corazón te entregas a la inteligencia; si llamas a la inteligencia y pides discernimiento; si la buscas como a la plata, como a un tesoro escondido, entonces comprenderás en temor del señor y hallaras el conocimiento de Dios. Porque el SEÑOR da la sabiduría; conocimiento y ciencia brotan de sus labios”

Proverbios 2:1-6

Gracias a Dios por darme la existencia y poder lograr mis sueños.

A mis padres por todos sus esfuerzos y apoyo brindados durante mi proceso de aprendizaje, y por contagiarme de su espíritu luchador.

A todos mis hermanos por su generosidad y confianza ofrecida en la realización de este proyecto

A todos los docentes por ser la guía en esta formación

A mis amigos, compañeros de especialización y demás familiares por su apoyo incondicional

MIRLEDIS ELENA MARTINEZ LEAL

DEDICATORIA

Este nuevo logro que alcanzo se lo dedico a Dios por ser quien guía cada uno de mis pasos y me ha regalado la salud y energías para salir adelante, a mis padres por ser mi apoyo, consejos e inspiración para salir adelante, a mis profesores y compañero por ayudarme a adquirir nuevos conocimientos y nuevas amistades que espero conservar por mucho tiempo mas y por ultimo pero no menos importante a Comfaguajira que me ayudo a cumplir este sueño dándome el espacio y oportunidad de crecer como persona y profesional.

ROSA ESTUPIÑAN MEJIA

CONTENIDO

	Pág.
RESUMEN	12
SUMARY	13
INTRODUCCIÓN	14
1. JUSTIFICACIÓN	16
2. PROBLEMA	18
2.1 PLANTEAMIENTO DEL PROBLEMA	18
2.2 FORMULACIÓN DEL PROBLEMA	18
3. OBJETIVOS	20
3.1 OBJETIVO GENERAL	20
3.2 OBJETIVOS ESPECÍFICOS	20
4. PROPÓSITOS DEL ESTUDIO	22
5. DELIMITACIÓN	23
5.1 DELIMITACIÓN TEMPORAL	23
5.2 DELIMITACIÓN GEOGRÁFICA	23
5.3 DELIMITACIÓN DE RECURSOS	23
5.4 DELIMITACIÓN TECNICA	23
6. MARCO TEÓRICO	24
6.1 MARCO CONCEPTUAL	31
6.2 MARCO REFERENCIAL	36
6.2.1 COBIT	36
6.2.2 CONTROL INTERNO	38
6.2.2.1 DEFINICION Y OBJETIVOS	38
6.2.2.2 COMPONENTES	40
6.2.2.3 AMBIENTE DE CONTROL	41
6.2.2.4 EVALUACION DE RIESGOS	43

6.2.2.5 ACTIVIDADES DE CONTROL	44
6.2.2.6 INFORMACION Y COMUNICACIÓN	46
6.3 MARCO LEGAL	50
6.3.1 REGLAMENTACIÓN LEGAL COLOMBIANA SOBRE LAS CAJAS DE COMPENSACIÓN FAMILIAR	51
6.3.2 REGULACIONES Y NORMAS QUE TRATAN EL RIESGO	50
6.3.3 ISO/IEC 27001	58
6.3.4 ISO/IEC 27005	58
6.3.5 Basilea II	58
6.3.6 Ley SarbanesOxley (SOX)	58
7. HIPOTESIS	59
8. DISEÑO METODOLÓGICO	60
8.1 TIPO DE INVESTIGACIÓN	60
8.2 POBLACIÓN	60
9. CRONOGRAMA DE ACTIVIDADES	61
10. LA ORGANIZACIÓN CAJA DE COMPESACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA” Y SU FUNCIONAMIENTO	62
10.1 ACTIVIDAD ECONOMICA DE LA EMPRESA	62
10.2 MISIÓN DE LA CAJA DE COMPESACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA”	62
10.3 VISIÓN DE LA CAJA DE COMPESACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA”	62
10.4.1 VALORES CORPORATIVOS DE LA CAJA DE COMPESACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA”	63
10.4.2 Ética	63
10.4.3 Trabajo en Equipo	63
10.4.4 Cultura del servicio	63
10.4.5 Innovación	63
10.5 GESTION TECNOLOGICA COMFAGUAJIRA	64

10.5.1	Objetivo	64
10.5.2	Alcance	65
10.5.3	Procesos Asociados	65
10.5.3.1	Logística	65
10.5.3.2	Planeación	65
10.6	ORGANIGRAMA DEL DEPARTAMENTO DE SISTEMAS DE COMFAGUAJIRA	65
10.7	MAPA DE PROCESO CORPORATIVO DE COMFAGUAJIRA	66
10.8	ACTIVOS DE TI	68
	METODOLOGIA	68
10.9	ACTIVIDADES	68
10.10	INVERSION	69
10.11	AUTODIAGNOSTICO MEDIANTE COSO DE LOS RIESGOS DE LA GESTION TECNOLOGICA COMFAGUAJIRA	70
10.11.1	Arquitectura de hardware	70
10.11.2	Plan estratégico de sistemas	71
10.11.3	Desarrollo de sistemas de información	71
10.11.4	Respaldo de la Información	72
10.11.5	Seguridad Física de la información	72
10.11.6	Seguridad Lógica de la información	73
10.12	RESULTADO DEL DIAGNOSTICO INICIAL DE RIESGO	76
10.13	VALORACIÓN DE LOS RIESGOS	78
10.13.1	MATRIZ DE CRITERIOS PARA CALIFICAR EL IMPACTO	78
10.13.2	MATRIZ DE CRITERIOS PARA CALIFICAR LA PROBABILIDAD	80
	CONCLUSIONES	81
	RECOMENDACIONES	83
	BIBLIOGRAFIA	86
	ANEXOS	87

LISTA DE GRAFICOS

	Pág.
GRAFICO 1. ORGANIGRAMA DEL DEPARTAMENTO DE SISTEMAS DE COMFAGUAJIRA.....	65
GRAFICO 2 . MAPA DE PROCESO CORPORATIVO DE COMFAGUAJIRA.....	66
GRAFICO 3. GESTION TECNOLOGICA.....	76

LISTA DE TABLA

	Pág.
TABLA 1. REGLAMENTACIÓN LEGAL COLOMBIANA SOBRE LAS CAJAS DE COMPENSACIÓN FAMILIAR.....	51
TABLA 2.CRONOGRAMA DE ACTIVIDADES.....	61
TABLA 3. LA ORGANIZACIÓN CAJA DE COMPEACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA” Y SU FUNCIONAMIENTO.....	62
TABLA 4. ACTIVOS DE TI.....	67
TABLA 5. INVERSION.....	69
TABLA 6. AUTODIAGNOSTICO MEDIANTE COSO DE LOS RIESGOS DE LA GESTION TECNOLÓGICA COMFAGUAJIRA.....	70
TABLA 7. VALORACION DE LOS RIESGOS.....	78

RESUMEN

Este proyecto fue realizado con el fin de ofrecerle a COMFAGUAJIRA, las herramientas necesarias para iniciar la implementación de la circular 023 de 2010 de la Superintendencia de Subsidio Familiar, la cual obliga a las cajas de compensación de Colombia a implementar un sistema de control interno en todos sus procesos entre los cuales esta la gestión tecnológica, con el fin de que estas implementen los siguientes conceptos:

AUTOGESTION: Capacidad de interpretar, coordinar, ejecutar y evaluar de manera efectiva, eficiente y eficaz su funcionamiento.

AUTOCONTROL: Capacidad de cada uno de los funcionarios para evaluar, mejorar y controlar su trabajo.

AUTOREGULACION: Capacidad de la entidad de aplicar métodos, normas y procedimientos que permitan el desarrollo, implementación y mejoramiento del Sistema de Control Interno.

SUMMARY

This project was undertaken to COMFAGUAJIRA offer the tools necessary to begin implementation of Circular 023 of 2010 of the Superintendency of Family Subsidy, which requires the compensation of Colombia to implement a system of internal control all the processes including the management of technology, so that these implement the following:

SELF MANAGEMENT: The ability to interpret, coordinate, implement and evaluate effective, efficient and effective functioning.

SELF CONTROL: The ability of each staff to evaluate, improve and control their work.

SELF REGULATION: The ability of the entity to apply methods, standards and procedures for developing, implementing and improving the System of Internal Control.

INTRODUCCIÓN

En la actualidad los cambios tecnológicos que ocurren, su complejidad y la velocidad con los que ocurren, son las raíces de la incertidumbre y el riesgo que las organizaciones confrontan. Las fusiones, la competencia global y los avances tecnológicos, las desregulaciones, y las nuevas regulaciones, el incremento en la demanda de los consumidores y de los habitantes, la responsabilidad social y ambiental de las organizaciones así como, la transparencia generan un ambiente operativo, cada día más riesgoso y complicado, surgiendo en adición nuevos retos con los cuales lidiar, resultado de los problemas que se presentan en las organizaciones que operan al margen de la ley o de conductas éticas.

Las Cajas de compensación familiar deben preservar la eficacia, eficiencia y efectividad de su gestión y capacidad operativa, así como salvaguardar los recursos públicos y privados que administran, para lo cual deberán contar con un sistema de administración de riesgos que permita la minimización de los costos y daños causados por éstos.

La administración de riesgos corporativos es un proceso efectuado por el directorio, administración y las personas de la organización, es aplicado desde la definición estratégica hasta las actividades del día a día, diseñado para identificar eventos potenciales que pueden afectar a la organización y administrar los riesgos dentro de su apetito, a objeto de proveer una seguridad razonable respecto del logro de los objetivos de la organización

Un sistema de gestión de riesgo se diseña con el único objetivo que las empresas sean más competitivas y productivas; siempre que las empresas adopten adecuadas herramientas, como la evaluación de las amenazas a causas de los riesgos, controles

utilizados para minimizar las amenazas o riesgos, La evaluación de los elementos del análisis de riesgos, se podrá lograr un verdadero sistema de prevención.

Este proyecto titulado *“Diseño del análisis de riesgo del proceso tecnológico de la caja de compensación familiar de la guajira “COMFAGUAJIRA”, para la aplicación del sistema de control interno subsidio familiar SCISF, según circular 0023 del 30 de noviembre de 2010 de la superintendencia de subsidio familiar,* busca solucionar o mitigar los riesgos encontrados en la empresa mencionada, mediante el diseño del análisis de riesgos. El producto de esta investigación contribuirá favorablemente a la empresa de la que se ocupa esta indagación, con excelentes resultados en la prevención o mitigación de los riesgos, realizando las actividades reguladas en la legislación colombiana.

En conclusión, el análisis de riesgos facilitará a COMFAGUAJIRA, la planeación, organización, ejecución, control y evaluación de los procedimientos que minimicen la ocurrencia de pérdidas o el impacto financiero, tecnológico, operativo y reputación de las pérdidas que puedan ocurrir.

1. JUSTIFICACION

La superintendencia del subsidio familiar busca que por medio de la aplicación de la circular 0023 del 30 de noviembre de 2010 en las cajas de compensación familiar de Colombia, apliquen la autorregulación, autogestión y autocontrol con el fin de implementar un sistema de control interno llamado SCISF (sistema de control interno del subsidio familiar), que les permita mejorar la eficiencia y eficacia en las operaciones, prevenir y mitigar la ocurrencia de fraudes, realizar una gestión adecuada de los riesgos, aumentar la confiabilidad y oportunidad en la información generada por la organización, adecuado cumplimiento de normatividad y regulaciones aplicables a la organización.¹

Dentro de los procesos para aplicar el sistema de control interno SCISF, se debe realizar un análisis de riesgo del proceso tecnológico de la caja, con base a los componentes de COSO: identificación de eventos, evaluación de riesgos y respuesta al riesgo.

Este análisis de riesgo es un proceso efectuado por la junta directiva, la gerencia y otro personal de la caja, aplicado en el establecimiento de estrategias a lo largo de la empresa, diseñado con el fin de establecer eventos potenciales que podrían afectar a la caja y administrar riesgos para alinearlos con el límite de riesgo aceptable, para proporcionar seguridad razonable respecto del logro de los objetivos estratégicos de la organización.

Los ejecutivos de la compañía deben definir y documentar las políticas de administración del riesgo, incluyendo sus objetivos, y su compromiso para ello. La política de administración del riesgo debe ser relevante dentro del contexto estratégico de la empresa, sus objetivos y metas, y la naturaleza del negocio.

¹<http://www.actualicese.com/normatividad/2010/11/30/circular-externa-0023-de-30-11-2010/>

La alta gerencia debe asegurarse que esta política es entendida, implantada y mantenida por todos los niveles de la organización.

Este proyecto está dirigido a la empresa CAJA DE COMPENSACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA”, dedicada a la protección a las familias de todo el departamento de la Guajira.

2. PROBLEMA

2.1 PLANTEAMIENTO DEL PROBLEMA

La superintendencia del subsidio familiar, profirió la circular externa n° 0023 del 30 de Noviembre de 2010, por medio de la cual instruye sobre el sistema de control interno que deben implementar las cajas de compensación familiar de Colombia, análisis de riesgo y comité independiente de auditoría SCISF ¹.

La superintendencia obliga a implementar y ajustar los elementos mínimos para crear un adecuado sistema de gestión de riesgo de acuerdo con las formalidades enmarcadas en los estándares internacionales como Cobit, ISO 27000, SOX, Coso, entre otros.

Para esto las cajas de compensación familiar de la guajira COMFAGUAJIRA, debe iniciar el diseño de sistema de control interno para la gestión de riesgos tecnológica, ya que esta es indispensable para el cumplimiento de los objetivos y la prestación de servicios de COMFAGUAJIRA en condiciones de seguridad, calidad y efectividad.

2.2 FORMULACION DEL PROBLEMA

El problema anteriormente expuesto se puede formular bajo las siguientes premisas:

¿De qué manera se puede aplicar el análisis de riesgo en la empresa “CAJA DE COMPEACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA”, de acuerdo con la CIRCULAR 0023 DEL 30 DE NOVIEMBRE DE 2010 DE LA SUPERINTENDENCIA DE SUBSIDIO FAMILIAR?

¿El análisis de riesgos de los procesos tecnológicos de COMFAGUAJIRA, puede ofrecerle a la gerencia de esta, el conocimiento necesario de los riesgos que enfrentan en la infraestructura tecnológica de la caja?

¿Cuáles son los estándares, buenas prácticas, normas y/o Guías para realizar el análisis de riesgos para los procesos tecnológicos de la caja?

OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar el análisis de riesgo del proceso tecnológico de la caja de compensación familiar de la guajira “COMFAGUAJIRA”, mediante el diagnóstico de la administración de los riesgos para la aplicación del sistema de control interno subsidio familiar SCISF, según circular 0023 del 30 de noviembre de 2010 de la superintendencia de subsidio familiar con el propósito de eliminar, mitigar o controlar los riesgos que afecten los procesos de la empresa

3.2 OBJETIVOS ESPECIFICOS.

1. Diagnosticar cómo se encuentra la empresa actualmente frente a los requerimientos de la circular 0023 del 30 de noviembre de 2010 de la superintendencia de subsidio familiar.
2. Definir los procesos tecnológicos de COMFAGUAJIRA que se le realizará el análisis y la evaluación de sus riesgos
3. Identificar los riesgos que afectan la gestión tecnológica de COMFAGUAJIRA
4. Valorar los riesgos identificados según su nivel de probabilidad de ocurrencia e impacto sobre la Caja.
5. Priorizar los riesgos según el nivel de severidad de los mismos
6. Elaborar la matriz de riesgo que le permita a la gerencia conocer el estado actual de sus riesgos en la gestión tecnológica

7. Elaborar las recomendaciones y las conclusiones generadas de todo el proceso de análisis de riesgos realizada.

3. PROPÓSITOS DEL ESTUDIO

Como propósito administrativo y empresarial se pretende dejar un Sistema de Gestión de riesgo del proceso tecnológico de la caja de compensación familiar de la guajira “COMFAGUAJIRA”, de tal manera que de ser implementado el sistema bajo las circular 023 de la superintendencia de subsidio familiar, la empresa pueda prestar un servicio con seguridad, calidad y efectividad.

El propósito investigativo es explorar un ente económico que presenta características particulares en la administración de los riesgos, conocer los riesgos que enfrentan la infraestructura tecnológica y establecer los aspectos más importantes a tener en cuenta para eliminar, mitigar o controlar los riesgos que afecten los procesos de la empresa.

A nivel académico se busca aplicar los conocimientos adquiridos en materias como la Gerencia de tecnología de la información, así como conocer profundamente el tema de los estándares internacionales como Cobit, ISO 27000, SOX, Coso, entre otros, que hoy en día cobran cada vez más importancia dentro de las empresas.

4. DELIMITACIÓN

5.1 DELIMITACIÓN TEMPORAL

Este proyecto se realizara en el periodo comprendido entre Junio y Octubre del 2011.

5.2 DELIMITACIÓN GEOGRÁFICA

La población objeto de estudio es la empresa CAJA DE COMPESACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA” ubicada en la ciudad de Riohacha, en la calle 13 No. 8 – 176.

5.3 DELIMITACIÓN DE RECURSOS

Para el diseño de este sistema de gestión de riesgo del proceso tecnológico en principio se utilizará información de la empresa y el de los trabajadores de la empresa de la caja de compensación familiar de la guajira “Comfaguajira” ubicada en la ciudad de Riohacha.

5.4 DELIMITACIÓN TECNICA

Este proyecto tiene como limitación los procesos tecnológicos de la CAJA DE COMPESACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA”

5. MARCO TEÓRICO

Con la responsabilidad reguladora cayendo sobre los ejecutivos durante toda la cadena de valor y el peligro de sanciones severas y variadas, la gestión de riesgos empresariales continúa creciendo en importancia dentro de todas las empresas

Al iniciar las actividades de una empresa sus directivos o dueños deben tener en cuenta que el riesgo estará presente en todo momento de su desarrollo, debido a diferentes factores como lo son: intensos cambios del entorno, la intensificación de la competencia, las reducción de las barreras de entrada, y obviamente la parte tecnológica que va avanzando a pasos agigantados. Para minimizar estos diferentes factores es que hace un tiempo se viene incorporando a las entidades la "Gestión de Riesgos", la que en nuestro país no está implantada en todos los sectores².

DEFINICION DE ERM

La administración del riesgo Empresarial (ERM) es un proceso, efectuado por la junta directiva de una entidad, su gerencia y otro personal, aplicado en el establecimiento de estrategias a lo largo de la empresa, diseñado para establecer eventos potenciales que podría afectar a la entidad y administrar riesgo para alinearlos con el límite de riesgo aceptable, para proporcionar seguridad razonable respecto del logro de los objetivos de la entidad.

GESTION DE RIESGOS

La Gestión de Riesgos es un proceso efectuado por el Consejo de Administración de una entidad, su Dirección y todo su restante personal, diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro

del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos.

La palabra "riesgo", ha tenido hasta la fecha muy diversas interpretaciones, en términos muy simples existe riesgo en cualquier situación en que no sabemos con exactitud lo que ocurrirá al futuro.

- Para "La International Organization for Standardization" (ISO) define al riesgo como:

"Combinación de la Probabilidad de un Evento y su Consecuencia" ISO aclara que el término riesgo es generalmente usado siempre y cuando exista la posibilidad de pérdidas (resultado negativo)".

- El "The Institute of Internal Auditors" (The IIA) define al riesgo como:

"La Posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos. El riesgo se mide en términos de impacto y probabilidad".

- Para otros autores, como los economistas rusos G. Goldstein y A. Gutz, lo definitivo en el riesgo es la incertidumbre. Según ellos el riesgo es "la incertidumbre en cuanto al potencial de pérdidas en el proceso de alcanzar los objetivos de la empresa

Beneficios de la Gestión de Riesgo.

La Gestión de Riesgos puede realizar una enorme contribución ayudando a la organización a gestionar los riesgos para poder alcanzar sus objetivos.

Los beneficios incluyen:

- Mayor posibilidad de alcanzar los objetivos;
- Consolida reportes de riesgos distintos a nivel de la Organización;

- Incrementa el entendimiento de riesgos claves y sus más amplias implicaciones;
- Identifica y comparte riesgos alrededor del negocio;
- Crea mayor enfoque de la gerencia en asuntos que realmente importan;
- Menos sorpresas y crisis;
- Mayor enfoque interno en hacer lo correcto en la forma correcta;
- Incrementa la posibilidad de que cambios en iniciativas puedan ser logrados;
- Capacidad de tomar mayor riesgo por mayores recompensas;
- Más información sobre riesgos tomados y decisiones realizadas

Algunas veces, el manejo de riesgos se centra en la contención de riesgo por causas físicas o legales (por ejemplo, desastres naturales o incendios, accidentes, muerte o demandas). Por otra parte, la gestión de riesgo financiero se enfoca en los riesgos que pueden ser manejados usando instrumentos financieros y comerciales.

² http://www.nodo50.org/cubasigloXXI/economia/gcueto_311206.pdf

PLANIFICACIÓN DE LA ADMINISTRACIÓN DE RIESGOS ³

La planificación de la administración de los riesgos es el proceso de decidir cómo enfocar y planear las actividades de la administración de riesgos para un proyecto, y su principal resultado es el plan de administración de riesgo. Un plan de administración de riesgos documenta los procedimientos para administrar los riesgos de un proyecto. Un plan de administración de riesgos resume cómo la administración de riesgos será ejecutada en un proyecto en particular. Los elementos que se deben incluir en un plan de administración de riesgos son:

METODOLOGÍA

Se debe establecer cómo la administración de riesgo que será ejecutada en el proyecto. Determinar qué herramientas y fuentes de información está disponible y aplicable.

- **Roles y responsabilidades:** Determinar quiénes son las personas responsables de implementar las tareas específicas y proporcionar los informes relacionados a la administración de riesgo.
- **Presupuesto y plazos:** Determinar cuáles son los costos y plazos estimados para ejecutar las tareas relacionadas con los riesgos.
- **Categoría de riesgos:** Determinar cuáles son las categorías de los riesgos que serán identificados.
- **Probabilidad de riesgo e impacto:** Cuáles son las probabilidades y los impactos de los riesgos que serán evaluados. Cuáles son las técnicas cualitativas o cuantitativas que serán utilizadas para evaluar los riesgos.

- **Documentación de los riesgos:** Determinar los formatos de los reportes y los procesos que serán utilizados para las actividades de la administración de riesgos.

IDENTIFICACIÓN DE RIESGOS

La identificación de riesgos es el proceso de comprender qué eventos potencialmente podría dañar o mejorar a un proyecto en particular. Es importante identificar los riesgos potenciales lo más pronto posible, pero también se debe continuar con la identificación de los riesgos basados en los cambios en el entorno del proyecto.

Se cuenta con varias herramientas y técnicas para identificar riesgos. Los administradores de proyectos a menudo empiezan el proceso de identificación de los riesgos revisando la documentación, y la información reciente e histórica relacionada a la organización, y los supuestos que pueden afectar el proyecto. Después de identificar los riesgos potenciales, los administradores del proyecto pueden utilizar diferentes técnicas para identificar los riesgos. Las cinco técnicas más utilizadas son: la tormenta de ideas, el método Delphi, las entrevistas, el análisis causa efecto, y el análisis FODA (Fortalezas, debilidades, oportunidades, y amenazas).

Análisis cualitativo de riesgos

El análisis cuantitativo de riesgos involucra evaluar la probabilidad y el impacto de la identificación de riesgos, para determinar su magnitud y prioridad. Para poder evaluar cuantitativamente los riesgos se cuenta fundamentalmente con tres herramientas: La matriz de probabilidad e impacto para calcular los factores de riesgos, la técnica de seguimiento de los diez factores de riesgo más importantes, y la evaluación del juicio de expertos.

Análisis cuantitativo de los riesgos

El análisis cuantitativo del riesgo a menudo sucede al análisis cualitativo del riesgo, aunque ambos procesos pueden llevarse por separado o en forma simultánea.

En algunos proyectos, el equipo puede solamente ejecutar el análisis cualitativo. La naturaleza del proyecto y la disponibilidad de tiempo y dinero influyen en el tipo de técnica a utilizar. Los proyectos grandes y complejos que involucran tecnología de punta requieren la aplicación de técnicas cuantitativas. Las principales técnicas para el análisis cuantitativo exigen la recolección de datos, la aplicación de técnicas cuantitativas, y técnicas de modelamiento. Las técnicas de análisis cuantitativo más utilizadas son: el análisis de árboles de decisión, la simulación, y el análisis de sensibilidad.

PLANIFICACIÓN DE LA RESPUESTA DE LOS RIESGOS

Después que una organización identifica y cuantifica los riesgos, debe desarrollar una apropiada estrategia para poder enfrentarlos.

Las cuatro estrategias de respuesta riesgos negativos son:

- a.** Evitar los riesgos o eliminar una amenaza específica, generalmente se logra al eliminar sus causas.
- b.** Aceptar los riesgos o aceptar las consecuencias si el riesgo ocurriese.
- c.** Transferir los riesgos o trasladar la consecuencia de un riesgo y la responsabilidad por su administración a terceros.

d. Mitigar los riesgos o reducir el impacto de un evento riesgoso al reducir la probabilidad de su ocurrencia.

Las cuatro estrategias para enfrentar los riesgos positivos son:

a. Explotación del riesgo para asegurarnos que el riesgo positivo ocurra.

b. Compartir el riesgo o asignar la propiedad del riesgo a un tercero.

c. Mejora del riesgo o cambiar el tamaño de la oportunidad al identificar y maximizar los inductores claves de un riesgo positivo.

d. Aceptar el riesgo también se aplica a los riesgos positivos cuando el equipo del proyecto no puede o escoge no tomar ninguna acción para enfrentar el riesgo.

Monitoreo y control de los riesgos.

El monitoreo y control de los riesgos involucra la ejecución de los procesos de la administración de riesgo para responder a los eventos riesgosos.

Ejecutar los procesos de la administración de riesgos significa asegurar que el reconocimiento de los riesgos es una actividad permanente ejecutada por todos los miembros del equipo a lo largo de la vida del proyecto.

Riesgo Tecnológico

El riesgo tecnológico es inherente a una falla, incumplimientos de seguridad o a otra deficiencia en las plataformas automáticas que brindan soporte al funcionamiento diario de la Entidad (sistemas de aplicaciones) y la infraestructura informática en la cual reside (centro de datos, redes y computadoras distribuidas). Estos riesgos se ven afectados por la implementación de cambios y la necesidad de renovar constantemente la cartera tecnológica de la entidad.

³ <http://www.scielo.org.pe/pdf/id/v9n1/a13v9n1.pdf>

6.1 MARCO CONCEPTUAL

GESTION DE RIESGO: Corresponde a la identificación, medición, control y monitoreo de los riesgos de manera transversal al interior de la organización – Despliegue organizacional y autocontrol.

GESTION DE TECNOLOGIA: Corresponde a la definición de políticas, procedimientos, riesgos y controles asociados con los procesos de tecnología de la información.

GESTION CONTABLE: Corresponde a la documentación de los procesos, riesgos y controles asociados con la generación y reporte de estados financieros de manera exacta, confiable y oportuna.

CIRCULAR 023: Son las instrucciones sobre el sistema de control interno en las cajas de compensación familiar, gestión de riesgo y comité independiente de Auditoria

AUTORREGULACION: Corresponde a la capacidad de la entidad de aplicar métodos, normas y procedimientos que permitan el desarrollo, implementación y mejoramiento del SCISF.

AUTOGESTION: Corresponde a la capacidad de interpretar, coordinar, ejecutar y evaluar de manera efectiva, eficiente y eficaz su funcionamiento.

AUTOCONTROL: Corresponde a la capacidad de cada uno de los funcionarios para evaluar, mejorar y controlar su trabajo.

MONITOREO: Corresponde a los procedimientos asociados con el autocontrol en cada uno de los procesos, las actividades ejecutadas a nivel de supervisión y los procedimientos ejecutados por los órganos de control.

SCISF: Sistema de control interno del subsidio familiar.

CONTROL INTERNO: Es un proceso, afectado por el comité directivo de una compañía, la administración y otro personal, diseñado para proporcionar seguridad razonable respecto a: Eficiencia y eficacia de las operaciones, confiabilidad de la información financiera y el cumplimiento de leyes y regulaciones aplicables de identificar, localizar y valorar los factores de riesgo de modo que se pueda actualizar periódicamente y que permita el diseño de medidas de intervención.

COSO: COMMITTEE OF SPONSORING ORGANIZATIONS

COBIT: Es un marco de referencia de gobierno de TI y un conjunto de herramientas de soporte que permite a los gerentes reducir la brecha entre los requerimientos de control, los temas técnico y los riesgos del negocio

AMBIENTE DE CONTROL: Corresponde a los elementos de la cultura organizacional que fomentan todos los integrantes (Principios, valores y conductas orientadas hacia el control). Es el fundamento de todos los demás elementos que componen el SCI.

ACTIVIDADES DE CONTROL: Corresponde a las actividades requeridas para administrar los riesgos de la entidad teniendo en cuenta los aspectos normativos, operativos y tecnológicos.

INFORMACIÓN: Corresponde al análisis de la información: criterios de seguridad (confidencialidad, integridad y disponibilidad), calidad (efectividad, eficiencia y

confiabilidad). Así mismo conocimiento de los controles específicos para la entrada el procesamiento y la salida de la información.

COMUNICACIÓN: Corresponde a los procedimientos asociados con la comunicación eficaz a través de la entidad desde el punto de vista interno y externo.

AUDITORÍA: Proceso sistemático independiente y documentado para obtener evidencias de la auditoria y evaluarla de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría.

CRONOGRAMA DE ACTIVIDADES: Registro pormenorizado del plan de acción del programa, ubicado en el tiempo y con la asignación de responsabilidades de ejecución. Se recomienda elaborarlo para un periodo máximo de un año.

ORGANIZACIÓN: compañía, corporación, firma, empresa, autoridad o institución, o parte o combinación de ellas, sean o no sociedades públicas o privadas, que tienen sus propias funciones y administración.

ACTIVO: Es un objeto o recurso de valor empleado en una empresa u organización.

STAKEHOLDERS: Personas, organizaciones entre otros, que pueden afectar o pueden verse afectadas por, o perciben pueden ser afectadas por una decisión, actividad o un riesgo.

AREAS DE IMPACTO: Es todo recurso, bien u oportunidad al cual la Organización le ha (o debe) asignar un valor y su afectación podría comprometer el cumplimiento de sus objetivos y metas, por tal motivo deben ser protegidas o maximizadas.

FUENTES DE RIESGOS: Es todo individuo, grupo humano, entidad, elemento físico, o fenómeno del entorno, de los cuales se pueden derivar eventos que podrían afectar las áreas de impacto (objetos en riesgo) de la organización, cuya ocurrencia se debe evitar (minimizar) o maximizar, para incrementar la posibilidad del logro de los objetivos y metas.

AMENAZA: Es un evento que puede causar un incidente de seguridad en una empresa u organización produciendo pérdidas o daños potenciales en sus activos.

VULNERABILIDAD: Es una debilidad que puede ser explotada con la materialización de una o varias amenazas a un activo.

EVENTO: Es la ocurrencia o cambio, de un particular conjunto de circunstancias.

CONSECUECIA: Es el resultado de un evento (Causa) expresado cualitativa o cuantitativamente, sea este una pérdida, perjuicio, desventaja o ganancia.

RIESGO: Es la probabilidad de ocurrencia de un evento que puede ocasionar un daño potencial a servicios, recursos o sistemas de una empresa.

PROBABILIDAD: Se utiliza como una descripción general de Probabilidad, Frecuencia o posibilidad.

PROBABILIDAD: Es la posibilidad de un evento específico o resultado, medido por la rata de eventos específicos o resultados sobre el número total de posibles eventos o resultados. (Rango de 0–1/%)

FRECUENCIA: Es una medida del coeficiente de ocurrencia de un evento expresado como la cantidad de ocurrencias de un evento en un tiempo dado. (Una vez cada día/Una vez cada semana/Una vez cada 15 días/Una vez cada mes.....)

POSIBILIDAD: Expresión cualitativa de la Probabilidad

ANÁLISIS: Examinar o descomponer un todo detallando cada uno de los elementos que lo forman a fin de terminar la relación entre sus principios y elementos.

CONTROL: Es un mecanismo de seguridad de prevención y corrección empleado para disminuir las vulnerabilidades.

CONTROLAR EL RIESGO: Fortalecer los controles existentes y/o agregar nuevos controles.

ELIMINAR EL RIESGO: Eliminar el activo relacionado y con ello se elimina el riesgo.

COMPARTIR EL RIESGO: Mediante acuerdos contractuales parte del riesgo se traspasa a un tercero.

ACEPTAR EL RIESGO: Se determina que el nivel de exposición es adecuado y por lo tanto se acepta.

ANÁLISIS DE RIESGO: Es el proceso cuantitativo o cualitativo que permite evaluar los riesgos. Esto involucra una estimación de incertidumbre del riesgo y su impacto.

ADMINISTRACIÓN DE RIESGO: Es la práctica de usar el análisis de riesgo para diseñar estrategias que permitan reducir o mitigar los riesgos

6.2 MARCO REFERENCIAL

6.2.1 COBIT ⁴

En años recientes, ha sido cada vez más evidente para los legisladores, usuarios y proveedores de servicios la necesidad de un Marco Referencial para la seguridad y el control de tecnología de información (TI). Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información (TI) relacionada. En esta sociedad global (donde la información viaja a través del “ciberespacio” sin las restricciones de tiempo, distancia y velocidad) esta criticidad emerge de:

- La creciente dependencia en información y en los sistemas que proporcionan dicha información
- La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las “ciber amenazas” y la guerra de información.
- La escala y el costo de las inversiones actuales y futuras en información y tecnología de información; y
- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos.

Para muchas organizaciones, la información y la tecnología que la soporta, representan los activos más valiosos de la empresa. Verdaderamente, la información y los sistemas de información son “penetrantes” en las organizaciones (desde la plataforma del usuario hasta las redes locales o amplias, cliente servidor y equipos Mainframe. Muchas organizaciones reconocen los beneficios potenciales que la tecnología puede proporcionar. Las organizaciones exitosas, sin embargo, también comprenden y administran los riesgos asociados con la implementación de nueva tecnología. Por lo

tanto, la administración debe tener una apreciación por, y un entendimiento básico de los riesgos y limitantes del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados la administración debe decidir la inversión razonable en seguridad y control en TI y cómo lograr un balance entre riesgos e inversiones en control en un ambiente de TI frecuentemente impredecible. La administración necesita un Marco Referencial de prácticas de seguridad y control de TI generalmente aceptadas para medir comparativamente su ambiente de TI, tanto el existente como el planeado. Existe una creciente necesidad entre los USUARIOS en cuanto a la seguridad en los servicios TI, a través de la acreditación y la auditoría de servicios de TI proporcionados internamente o por terceras partes, que aseguren la existencia de controles adecuados. Actualmente, sin embargo, es confusa la implementación de buenos controles de TI en sistemas de negocios por parte de entidades comerciales, entidades sin fines de lucro o entidades gubernamentales. Esta confusión proviene de los diferentes métodos de evaluación, tales como ITSEC, TCSEC, evaluaciones ISO9000, nuevas evaluaciones de control interno COSO, etc. Como resultado, los usuarios necesitan una base general a ser establecida como primer paso. Frecuentemente, los AUDITORES han tomado el liderazgo en estos esfuerzos internacionales de estandarización, debido a que ellos enfrentan continuamente la necesidad de sustentar y apoyar frente a la Gerencia su opinión acerca de los controles internos. Sin contar con un marco referencial, ésta se convierte en una tarea demasiado complicada. Esto ha sido mostrado en varios estudios recientes acerca de la manera en laque los auditores evalúan situaciones complejas de seguridad y control en TI, estudios que fueron dados a conocer casi simultáneamente en diferentes partes del mundo. Incluso, la administración consulta cada vez más a los auditores para que la asesoren en forma proactiva en lo referente a asuntos de seguridad y control de TI.

⁴ <http://www.slideshare.net/comik7/m-a-r-c-o-d-e-r-e-f-e-r-e-n-c-i-a-c-o-b-i-t-2287352>

6.2.2 CONTROL INTERNO ⁵

Publicado en EE.UU. en 1992, surgió como una respuesta a las inquietudes que planteaban la diversidad de conceptos, definiciones e interpretaciones existentes en torno a la temática referida.

Plasma los resultados de la tarea realizada durante más de cinco años por el grupo de trabajo que la TREADWAY COMMISSION, NATIONAL COMMISSION ON FRAUDULENT FINANCIAL REPORTING creó en Estados Unidos en 1985 bajo la sigla COSO (COMMITTEE OF SPONSORING ORGANIZATIONS). El grupo estaba constituido por representantes de las siguientes organizaciones:

- American Accounting Association (AAA)
- American Institute of Certified Public Accountants (AICPA)
- Financial Executive Institute (FEI)
- Institute of Internal Auditors (IIA)
- Institute of Management Accountants (IMA)
- La redacción del informe fue encomendada a Coopers&Lybrand.

Se trataba entonces de materializar un objetivo fundamental: definir un nuevo marco conceptual del control interno, capaz de integrar las diversas definiciones y conceptos que venían siendo utilizados sobre este tema, logrando así que, al nivel de las organizaciones públicas o privadas, de la auditoría interna o externa, o de los niveles académicos o legislativos, se cuente con un marco conceptual común, una visión integradora que satisfaga las demandas generalizadas de todos los sectores involucrados.

6.2.2.1 DEFINICION Y OBJETIVOS

El Control Interno es un proceso integrado a los procesos, y no un conjunto de pesados mecanismos burocráticos añadidos a los mismos, efectuado por el consejo de la administración, la dirección y el resto del personal de una entidad, diseñado con el

objeto de proporcionar una garantía razonable para el logro de objetivos incluidos en las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes, reglamentos y políticas.

Completan la definición algunos conceptos fundamentales:

- El control interno es un proceso, es decir un medio para alcanzar un fin y no un fin en sí mismo.
- Lo llevan a cabo las personas que actúan en todos los niveles, no se trata solamente de manuales de organización y procedimientos.
- Sólo puede aportar un grado de seguridad razonable, no la seguridad total, a la conducción.
- Está pensado para facilitar la consecución de objetivos en una o más de las categorías señaladas las que, al mismo tiempo, suelen tener puntos en común.

Al hablarse del control interno como un proceso, se hace referencia a una cadena de acciones extendida a todas las actividades, inherentes a la gestión e integrados a los demás procesos básicos de la misma: planificación, ejecución y supervisión. Tales acciones se hallan incorporadas (no añadidas) a la infraestructura de la entidad, para influir en el cumplimiento de sus objetivos y apoyar sus iniciativas de calidad.

Según la Comisión de Normas de Control Interno de la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI), el control interno puede ser definido como el plan de organización, y el conjunto de planes, métodos, procedimientos y otras medidas de una institución, tendientes a ofrecer una garantía razonable de que se cumplan los siguientes objetivos principales:

- Promover operaciones metódicas, económicas, eficientes y eficaces, así como productos y servicios de la calidad esperada.

- Preservar al patrimonio de pérdidas por despilfarro, abuso, mala gestión, errores, fraudes o irregularidades.
- Respetar las leyes y reglamentaciones, como también las directivas y estimular al mismo tiempo la adhesión de los integrantes de la organización a las políticas y objetivos de la misma.
- Obtener datos financieros y de gestión completos y confiables y presentados a través de informes oportunos.

Para la alta dirección es primordial lograr los mejores resultados con economía de esfuerzos y recursos, es decir al menor costo posible. Para ello debe controlarse que sus decisiones se cumplan adecuadamente, en el sentido que las acciones ejecutadas se correspondan con aquéllas, dentro de un esquema básico que permita la iniciativa y contemple las circunstancias vigentes en cada momento.

Por consiguiente, siguiendo los lineamientos de INTOSAI, incumbe a la autoridad superior la responsabilidad en cuanto al establecimiento de una estructura de control interno idónea y eficiente, así como su revisión y actualización periódica.

Ambas definiciones (COSO e INTOSAI) se complementan y conforman una versión amplia del control interno: la primera enfatizando respecto a su carácter de proceso constituido por una cadena de acciones integradas a la gestión, y la segunda atendiendo fundamentalmente a sus objetivos.

6.2.2.2 COMPONENTES

El marco integrado de control que plantea el informe COSO consta de cinco componentes interrelacionados, derivados del estilo de la dirección, e integrados al proceso de gestión:

- Ambiente de control
- Evaluación de riesgos
- Actividades de control

- Información y comunicación
- Supervisión

El ambiente de control refleja el espíritu ético vigente en una entidad respecto del comportamiento de los agentes, la responsabilidad con que encaran sus actividades, y la importancia que le asignan al control interno.

Sirve de base de los otros componentes, ya que es dentro del ambiente reinante que se evalúan los riesgos y se definen las actividades de control tendientes a neutralizarlos. Simultáneamente se capta la información relevante y se realizan las comunicaciones pertinentes, dentro de un proceso supervisado y corregido de acuerdo con las circunstancias.

El modelo refleja el dinamismo propio de los sistemas de control interno. Así, la evaluación de riesgos no sólo influye en las actividades de control, sino que puede también poner de relieve la conveniencia de reconsiderar el manejo de la información y la comunicación.

No se trata de un proceso en serie, en el que un componente incide exclusivamente sobre el siguiente, sino que es interactivo multidireccional en tanto cualquier componente puede influir, y de hecho lo hace, en cualquier otro.

Existe también una relación directa entre los objetivos (Eficiencia de las operaciones, confiabilidad de la información y cumplimiento de leyes y reglamentos) y los cinco componentes referenciados, la que se manifiesta permanentemente en el campo de la gestión: las unidades operativas y cada agente de la organización conforman secuencialmente un esquema orientado a los resultados que se buscan, y la matriz constituida por ese esquema es a su vez cruzada por los componentes.

6.2.2.3 AMBIENTE DE CONTROL

El ambiente de control define al conjunto de circunstancias que enmarcan el accionar de una entidad desde la perspectiva del control interno y que son por lo tanto

determinantes del grado en que los principios de este último imperan sobre las conductas y los procedimientos organizacionales.

Es, fundamentalmente, consecuencia de la actitud asumida por la alta dirección, la gerencia, y por carácter reflejo, los demás agentes con relación a la importancia del control interno y su incidencia sobre las actividades y resultados.

Fija el tono de la organización y, sobre todo, provee disciplina a través de la influencia que ejerce sobre el comportamiento del personal en su conjunto.

Constituye el andamiaje para el desarrollo de las acciones y de allí deviene su trascendencia, pues como conjunción de medios, operadores y reglas previamente definidas, traduce la influencia colectiva de varios factores en el establecimiento, fortalecimiento o debilitamiento de políticas y procedimientos efectivos en una organización.

Los principales factores del ambiente de control son:

- La filosofía y estilo de la dirección y la gerencia.
- La estructura, el plan organizacional, los reglamentos y los manuales de procedimiento.
- La integridad, los valores éticos, la competencia profesional y el compromiso de todos los componentes de la organización, así como su adhesión a las políticas y objetivos establecidos.
- Las formas de asignación de responsabilidades y de administración y desarrollo del personal.
- El grado de documentación de políticas y decisiones, y de formulación de programas que contengan metas, objetivos e indicadores de rendimiento.

En las organizaciones que lo justifiquen, la existencia de consejos de administración y comités de auditorías con suficiente grado de independencia y calificación profesional.

El ambiente de control reinante será tan bueno, regular o malo como lo sean los factores que lo determinan. El mayor o menor grado de desarrollo y excelencia de éstos hará, en ese mismo orden, a la fortaleza o debilidad del ambiente que generan y consecuentemente al tono de la organización.

6.2.2.4 EVALUACION DE RIESGOS

El control interno ha sido pensado esencialmente para limitar los riesgos que afectan las actividades de las organizaciones. A través de la investigación y análisis de los riesgos relevantes y el punto hasta el cual el control vigente los neutraliza se evalúa la vulnerabilidad del sistema. Para ello debe adquirirse un conocimiento práctico de la entidad y sus componentes de manera de identificar los puntos débiles, enfocando los riesgos tanto a los niveles de la organización (internos y externos) como de la actividad.

El establecimiento de objetivos es anterior a la evaluación de riesgos. Si bien aquéllos no son un componente del control interno, constituyen un requisito previo para el funcionamiento del mismo.

Los objetivos (relacionados con las operaciones, con la información financiera y con el cumplimiento), pueden ser explícitos o implícitos, generales o particulares. Estableciendo objetivos globales y por actividad, una entidad puede identificar los factores críticos del éxito y determinar los criterios para medir el rendimiento.

A este respecto cabe recordar que los objetivos de control deben ser específicos, así como adecuados, completos, razonables e integrados a los globales de la institución.

Una vez identificados, el análisis de los riesgos incluirá:

- Una estimación de su importancia / trascendencia.
- Una evaluación de la probabilidad / frecuencia.
- Una definición del modo en que habrán de manejarse.

Dado que las condiciones en que las entidades se desenvuelven suelen sufrir variaciones, se necesitan mecanismos para detectar y encarar el tratamiento de los riesgos asociados con el cambio. Aunque el proceso de evaluación es similar al de los otros riesgos, la gestión de los cambios merece efectuarse independientemente, dada su gran importancia y las posibilidades de que los mismos pasen inadvertidos para quienes están inmersos en las rutinas de los procesos.

Existen circunstancias que pueden merecer una atención especial en función del impacto potencial que plantean:

- Cambios en el entorno.
- Redefinición de la política institucional.
- Reorganizaciones o reestructuraciones internas.
- Ingreso de empleados nuevos, o rotación de los existentes.
- Nuevos sistemas, procedimientos y tecnologías.
- Aceleración del crecimiento.
- Nuevos productos, actividades o funciones.

Los mecanismos para prever, identificar y administrar los cambios deben estar orientados hacia el futuro, de manera de anticipar los más significativos a través de sistemas de alarma complementados con planes para un abordaje adecuado de las variaciones.

6.2.2.5 ACTIVIDADES DE CONTROL

Están constituidas por los procedimientos específicos establecidos como un reaseguro para el cumplimiento de los objetivos, orientados primordialmente hacia la prevención y neutralización de los riesgos.

Las actividades de control se ejecutan en todos los niveles de la organización y en cada una de las etapas de la gestión, partiendo de la elaboración de un mapa de riesgos según lo expresado en el punto anterior: conociendo los riesgos, se disponen los

controles destinados a evitarlos o minimizarlos, los cuales pueden agruparse en tres categorías, según el objetivo de la entidad con el que estén relacionados:

- Las operaciones
- La confiabilidad de la información financiera
- El cumplimiento de leyes y reglamentos

En muchos casos, las actividades de control pensadas para un objetivo suelen ayudar también a otros: los operacionales pueden contribuir a los relacionados con la confiabilidad de la información financiera, éstas al cumplimiento normativo, y así sucesivamente.

A su vez en cada categoría existen diversos tipos de control:

- Preventivo / Correctivos
- Manuales / Automatizados o informáticos
- Gerenciales o directivos

En todos los niveles de la organización existen responsabilidades de control, y es preciso que los agentes conozcan individualmente cuales son las que les competen, debiéndose para ello explicitar claramente tales funciones.

La gama que se expone a continuación muestra la amplitud abarcativa de las actividades de control, pero no constituye la totalidad de las mismas:

- Análisis efectuados por la dirección.
- Seguimiento y revisión por parte de los responsables de las diversas funciones o actividades.
- Comprobación de las transacciones en cuanto a su exactitud, totalidad, y autorización pertinente: aprobaciones, revisiones, cotejos, recálculos, análisis de consistencia, pre numeraciones.
- Controles físicos patrimoniales: arqueos, conciliaciones, recuentos.

- Dispositivos de seguridad para restringir el acceso a los activos y registros.
- Segregación de funciones.
- Aplicación de indicadores de rendimiento.

Es necesario remarcar la importancia de contar con buenos controles de las tecnologías de información, pues éstas desempeñan un papel fundamental en la gestión, destacándose al respecto el centro de procesamiento de datos, la adquisición, implantación y mantenimiento del software, la seguridad en el acceso a los sistemas, los proyectos de desarrollo y mantenimiento de las aplicaciones.

A su vez los avances tecnológicos requieren una respuesta profesional calificada y anticipativa desde el control.

6.2.2.6 INFORMACION Y COMUNICACIÓN

Así como es necesario que todos los agentes conozcan el papel que les corresponde desempeñar en la organización (funciones, responsabilidades), es imprescindible que cuenten con la información periódica y oportuna que deben manejar para orientar sus acciones en consonancia con los demás, hacia el mejor logro de los objetivos.

La información relevante debe ser captada, procesada y transmitida de tal modo que llegue oportunamente a todos los sectores permitiendo asumir las responsabilidades individuales.

La información operacional, financiera y de cumplimiento conforma un sistema para posibilitar la dirección, ejecución y control de las operaciones.

Está conformada no sólo por datos generados internamente sino por aquellos provenientes de actividades y condiciones externas, necesarios para la toma de decisiones.

Los sistemas de información permiten identificar, recoger, procesar y divulgar datos relativos a los hechos o actividades internas y externas, y funcionan muchas veces

como herramientas de supervisión a través de rutinas previstas a tal efecto. No obstante resulta importante mantener un esquema de información acorde con las necesidades institucionales que, en un contexto de cambios constantes, evolucionan rápidamente. Por lo tanto deben adaptarse, distinguiendo entre indicadores de alerta y reportes cotidianos en apoyo de las iniciativas y actividades estratégicas, a través de la evolución desde sistemas exclusivamente financieros a otros integrados con las operaciones para un mejor seguimiento y control de las mismas.

Ya que el sistema de información influye sobre la capacidad de la dirección para tomar decisiones de gestión y control, la calidad de aquél resulta de gran trascendencia y se refiere entre otros a los aspectos de contenido, oportunidad, actualidad, exactitud y accesibilidad.

La comunicación es inherente a los sistemas de información. Las personas deben conocer a tiempo las cuestiones relativas a sus responsabilidades de gestión y control. Cada función ha de especificarse con claridad, entendiendo en ello los aspectos relativos a la responsabilidad de los individuos dentro del sistema de control interno.

Asimismo el personal tiene que saber cómo están relacionadas sus actividades con el trabajo de los demás, cuáles son los comportamientos esperados, de qué manera deben comunicar la información relevante que generen.

Los informes deben transferirse adecuadamente a través de una comunicación eficaz. Esto es, en el más amplio sentido, incluyendo una circulación multidireccional de la información: ascendente, descendente y transversal.

La existencia de líneas abiertas de comunicación y una clara voluntad de escuchar por parte de los directivos resultan vitales.

Además de una buena comunicación interna, es importante una eficaz comunicación externa que favorezca el flujo de toda la información necesaria, y en ambos casos importa contar con medios eficaces, dentro de los cuales tan importantes como los

manuales de políticas, memorias, difusión institucional, canales formales e informales, resulta la actitud que asume la dirección en el trato con sus subordinados. Una entidad con una historia basada en la integridad y una sólida cultura de control no tendrá dificultades de comunicación. Una acción vale más que mil palabras.

6.2.2.7 SUPERVISION

Incumbe a la dirección la existencia de una estructura de control interno idónea y eficiente, así como su revisión y actualización periódica para mantenerla en un nivel adecuado. Procede la evaluación de las actividades de control de los sistemas a través del tiempo, pues toda organización tiene áreas donde los mismos están en desarrollo, necesitan ser reforzados o se impone directamente su reemplazo debido a que perdieron su eficacia o resultaron inaplicables. Las causas pueden encontrarse en los cambios internos y externos a la gestión que, al variar las circunstancias, generan nuevos riesgos a afrontar.

El objetivo es asegurar que el control interno funciona adecuadamente, a través de dos modalidades de supervisión: actividades continuas o evaluaciones puntuales.

Las primeras son aquellas incorporadas a las actividades normales y recurrentes que, ejecutándose en tiempo real y arraigadas a la gestión, generan respuestas dinámicas a las circunstancias sobrevinientes.

En cuanto a las evaluaciones puntuales, corresponden las siguientes consideraciones:

- a) Su alcance y frecuencia están determinados por la naturaleza e importancia de los cambios y riesgos que éstos conllevan, la competencia y experiencia de quienes aplican los controles, y los resultados de la supervisión continuada.
- b) Son ejecutados por los propios responsables de las áreas de gestión (autoevaluación), las auditorías internas (incluidas en el planeamiento o solicitadas especialmente por la dirección), y los auditores externos.

c) Constituyen en sí todo un proceso dentro del cual, aunque los enfoques y técnicas varíen, priman una disciplina apropiada y principios insoslayables.

La tarea del evaluador es averiguar el funcionamiento real del sistema: que los controles existan y estén formalizados, que se apliquen cotidianamente como una rutina incorporada a los hábitos, y que resulten aptos para los fines perseguidos.

d) Responden a una determinada metodología, con técnicas y herramientas para medir la eficacia directamente o a través de la comparación con otros sistemas de control probadamente buenos.

e) El nivel de documentación de los controles varía según la dimensión y complejidad de la entidad.

Existen controles informales que, aunque no estén documentados, se aplican correctamente y son eficaces, si bien un nivel adecuado de documentación suele aumentar la eficiencia de la evaluación, y resulta más útil al favorecer la comprensión del sistema por parte de los empleados. La naturaleza y el nivel de la documentación requieren mayor rigor cuando se necesite demostrar la fortaleza del sistema ante terceros.

f) Debe confeccionarse un plan de acción que contemple:

- El alcance de la evaluación
- Las actividades de supervisión continuadas existentes.
- La tarea de los auditores internos y externos.
- Áreas o asuntos de mayor riesgo.
- Programa de evaluaciones.
- Evaluadores, metodología y herramientas de control.
- Presentación de conclusiones y documentación de soporte
- Seguimiento para que se adopten las correcciones pertinentes.

Las deficiencias o debilidades del sistema de control interno detectadas a través de los diferentes procedimientos de supervisión deben ser comunicadas a efectos de que se adopten las medidas de ajuste correspondientes.

Según el impacto de las deficiencias, los destinatarios de la información pueden ser tanto las personas responsables de la función o actividad implicada como las autoridades superiores.

⁵ <http://www.iaia.org.ar/revistas/normaria/Normaria09.pdf>

6.3 MARCO LEGAL

Las cajas de compensaciones en los últimos años ha sido un tema de vital importancia para los gobiernos, es por ello que se han venido creando leyes, decretos y resoluciones que le han otorgado estructura a la Gestión de riesgos en Colombia. Es responsabilidad de la gerencia de la CAJA DE COMPESACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA”. La aplicación y concientización de estas legislaciones debido a que son el pilar para las políticas de una organización

La reglamentación en Colombia sobre las cajas de compensaciones es la Circular externa 023 de diciembre 12 de 2003 Superintendencia del Subsidio Familiar.

A continuación se describen los principales Decretos y Resoluciones que reglamentan las cajas de compensaciones.

6.3.1 REGLAMENTACIÓN LEGAL COLOMBIANA SOBRE LAS CAJAS DE COMPENSACIÓN FAMILIAR ⁶

LEY / AÑO	CONTENIDO
Ley 21 de enero 22 de 1982	Modifica el régimen del subsidio familiar
Decreto 341 de febrero 25 de 1988	Reglamenta ley 21 de 1982
Ley 89 de diciembre 29 de 1988	Asigna recursos al ICBF y el modo de recaudo
Decreto 784 de abril 18 de 1989	Reglamenta leyes 21/82 y 71/88

Ley 100 de enero 1 de 1993	Crea el sistema de seguridad social integral
Ley 119 de febrero 9 de 1994	Reestructura régimen del Sena
Ley 344 de diciembre 27 de 1996	Racionaliza gasto público e incluye factores para el cálculo de parafiscales
Decreto 1406 de julio 28 de 1999	Registro único de aportantes al sistema de seguridad social
Ley 550 de diciembre 30 de 1999	Intervención económica
Ley 590 de julio 10 de 2000	Mi pymes
Ley 789 de diciembre 27 de 2002	Apoyo al empleo, amplía la protección social y modifica el código laboral
Decreto 933 de abril 11 de 2003	Reglamenta contrato aprendiz ley 789/02
Decreto 827 de abril 24 de 2003	Reglamenta control de las cajas según ley 789/02

Decreto 1769 de junio 26 de 2003	Regula cuota monetaria de referencia ley 789/02
Ley 828 de julio 14 de 2003	Control a evasión en sistema de la seguridad social
Resolución 215 de julio 31 de 2003	Determina cuota monetaria de referencia desde el 2003
Decreto 2286 de agosto 12 de 2003	Reglamenta artículo 13 ley 789/02
Decreto 2340 de agosto 19 de 2003	Reglamento para la suspensión y expulsión de afiliados al sistema de compensación familiar
Decreto 2585 de septiembre 12 de 2003	Adiciona el decreto 933/03
Decreto 3450 del 2 de diciembre de 2003	Modifica arts. 12 y 13 del decreto 2340/03
Circular externa 023 de diciembre 12 de 2003 Superintendencia del Subsidio Familiar	Control y aplicación de la ley 789/02

Decreto 586 de marzo 1 de 2004	Modifica decreto 2340/03 subsidio al desempleo
Ley 905 de agosto 4 de 2004	Modifica ley 590 de 2000 Mi pymes
Decreto 2879 de septiembre 7 de 2004	Control a las C.T.A. y E.A.T.
Decreto 2996 de septiembre 16 de 2004	Modifica decreto 2879/2004
Decreto 3555 de octubre 28 de 2004	Modifica decreto 2996/04
Decreto 3667 de noviembre 8 de 2004	Dispone pago integrado aportes y parafiscales sistema seguridad social
Resolución 195 de febrero 7 de 2005	Determina la cuota monetaria de referencia del 2005
Directiva Presidencial 04 de mayo 4 de 2005	Pago integrado de aportes Entidades orden nacional
Decreto 1464 de mayo 10 de 2005	Fecha pago integrado aportes sistema seguridad social

Decreto 1465 de mayo 10 de 2005	Formulario pago integrado aportes seguridad social
Resolución 1303 de mayo 12 de 2005	Contenido formulario pago integrado aportes
Decreto 2233 de 2005	Reglamentación sobre el pago integrado de aportes a la seguridad social
Resolución 2310 de julio 22 de 2005	Modifica resolución 1303 de 2005
Ley 979 de julio 26 de 2005	Modifica parcialmente ley 54 de 1990
Instructivo 13 de agosto 1 de 2005 de Superintendente de notariado y registro sobre aplicación ley 962 de 2005 o anti trámites	
Resolución 634 de marzo 6 de 2006	Deroga resolución 1303 de 2005
Resolución 1317 de abril 25 de 2006	Modifica resolución 634 de 2006
Decreto 1931 de junio 12 de 2006	Reglamenta las fechas a partir de las cuales es obligatorio el uso de la Planilla Integrada para los empleadores
Resolución 2145 de junio 22 de 2006	Planilla integrada pago de aportes a la

	seguridad social de pensionados
Decreto 4588 de diciembre 14 de 2006	Reglamenta los pres y cooperativas de trabajo asociado.
Resolución 01190 de abril 24 de 2007	Modifica Resolución 736 de 2007
Circular Externa 012 de abril 30 de 2007	Instruye sobre Decreto 4588 de 2006
Decreto 1670 de mayo 14 de 2007	Modifica decreto 1406 de 1999
Decreto 2417 de junio 26 de 2007	Modifica decreto 4588 de 2006
Circular Externa 017 de julio 24 de 2007	Instruye sobre circular Externa 012 de 2007
Resolución 3975 de octubre 31 de 2007	Modifica plazos establecidos mediante decretos 1670 y 3085 de 2007
Decreto 400 de febrero 13 de 2008	Reglamenta numeral 3.3 del artículo 6° de ley 1151 de 2007
Decreto 728 de marzo 7 de 2008	Modifica obligatoriedad del uso del PILA por los pequeños aportantes y los independientes
Decreto 525 de febrero 23 de 2009	Reglamenta el artículo 43 de la Ley 590 de 2000

Ley 1438 de 2011	Reforma en salud
Decreto 545 de 2011	Reglamenta parcialmente los artículos 5°, 7°, 48 y 50 de la Ley 1429 de 2010
Ley 1429 de 2010	Formalización y Generación de Empleo
Decreto 2025 de junio 8 de 2011	Pre cooperativas y Cooperativas de trabajo asociado

⁶ <http://www.comfama.com/contenidos/servicios/Subsidio/Marco%20legal/marcolegal.asp>

6.3.2 REGULACIONES Y NORMAS QUE TRATAN EL RIESGO

Comunicación “A” 4609 del BCRA para entidades Financieras • Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información.

6.3.2.1 ISO/IEC 27001 Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI)

6.3.2.2 ISO/IEC 27005 Esta Norma proporciona directrices para la Gestión del riesgo de Seguridad de la Información en una Organización. Sin embargo, esta Norma no proporciona ninguna metodología específica para el análisis y la gestión del riesgo de la seguridad de la información.

6.3.2.3 Basilea II Estándar internacional que sirva de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios, para asegurar la protección de las entidades frente a los riesgos financieros y operativos.

6.3.2.4 Ley SarbanesOxley (SOX) Impulsada por el gobierno norteamericano como respuesta a los mega fraudes corporativos que impulsaron Enron, Tyco International, WorldCom y Peregrine Systems. Es un conjunto de medidas tendientes a asegurar la efectividad de los controles internos sobre reportes financieros.

6. HIPOTESIS

¿La disminución de los riesgos del proceso tecnológico de la caja, le daría a la organización un aumento de la productividad, eficacia, eficiencia y efectividad de su gestión y capacidad operativa, satisfacción de los empleados en su ambiente de trabajo y una mayor rentabilidad?

¿Con el diseño del análisis de riesgo del proceso tecnológico de la caja de compensación familiar de la guajira “COMFAGUAJIRA”, para la aplicación del sistema de control interno subsidio familiar SCISF, según circular 0023 del 30 de noviembre de 2010 de la superintendencia de subsidio familiar, la caja mejoraría sus procesos tecnológicos, tendrá mayor competitividad en el mercado y tendría una disminución en el impacto y la probabilidad de ocurrencia de los riesgos que la amenazan?

7. DISEÑO METODOLOGICO

8.1 TIPO DE INVESTIGACION

Para el conocimiento de los hechos se empleó el tipo de investigación descriptivo ya que se centra en la observación y descripción de la seguridad del entorno así como en las actividades diarias que puedan comprometer los procesos tecnológicos de la CAJA DE COMPESACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA”.

8.2 POBLACIÓN

En la práctica se acudió a la empresa CAJA DE COMPESACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA”, para observar los procesos tecnológicos, y poder estudiar, analizar, solucionar o mitigar los riesgos encontrados en la empresa.

8. CRONOGRAMA DE ACTIVIDADES																				
ACTIVIDADES - MESES	JUNIO	JUNIO				JULIO				AGOSTO				SEPT.				OCT.		
	SEMANA	SEMANA				SEMANA				SEMANA				SEMANA				SEMANA		
	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3
1. Etapa: Elaboración de la Propuesta																				
a. Identificar el Problema																				
b. Consulta Bibliográfica																				
c. Planteamiento y Definición del Problema																				
d. Definición de Objetivos y Justificación																				
e. Revisión por parte del Director																				
2. Etapa del anteproyecto																				
a. Elaboración del Marco Teórico y conceptual																				
b. Selección y estudio de la Metodología a seguir																				
c. Estimación de tiempo y recursos																				
d. Revisión por parte del Director																				
3. Etapa Diseño Sistema de Gestión de riesgos																				
a. Elaboración de preliminares																				
b. Diligenciamiento de los formatos y Entrevista																				
c. Estructura de Capítulos																				
d. Diseño Final																				
e. Revisión por parte del Director																				
f. Revisión y aprobación de evaluadores																				

10. LA ORGANIZACIÓN CAJA DE COMPESACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA” Y SU FUNCIONAMIENTO

10.1 ACTIVIDAD ECONOMICA DE LA EMPRESA

IDENTIFICACIÓN	
RAZON SOCIAL:	CAJA DE COMPESACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA”
NIT:	892.115.006 -5
SECTOR ECONOMICO:	PRIVADO
REPRESENTANTE LEGAL:	LUIS EDUARDO MEDINA ROMERO
Ubicación de CAJA DE COMPESACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA” está ubicada en la ciudad de Riohacha en la calle 13 No. 8 – 176. El trabajo realizado para dicha empresa corresponde al Trabajo de Grado de las Ingenieras: Rosa Estupiñan Mejía y Mirledis Martínez Leal.	

10.2 MISIÓN DE LA CAJA DE COMPESACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA”

Contribuir al mejoramiento de la calidad de vida de los trabajadores afiliados y sus familias y generar valor para la comunidad a través de la prestación de servicios sociales para ayudar al logro del equilibrio social en el Departamento de La Guajira.

10.3 VISIÓN DE LA CAJA DE COMPESACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA”

Ser una organización de clase mundial, reconocida y diferenciada por la calidad del servicio, innovación permanente, solidez económica y rentabilidad social.

10.4 VALORES CORPORATIVOS DE LA CAJA DE COMPESACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA”

10.4.1 Ética

Nuestro actuar cotidiano y desempeño laboral está orientado hacia el bien, basado en un conjunto de normas comportamientos y principios establecidos por la moral y las buenas costumbres.

10.4.2 Trabajo en Equipo

Somos un equipo con roles bien definidos. Compartimos responsabilidades, unimos fuerzas, hablamos el mismo lenguaje empresarial y estamos comprometidos con objetivos comunes.

10.4.3 Cultura del Servicio

Nos apasiona la gente. Disfrutamos servir. Brindamos respuesta efectiva a los requerimientos de los clientes, para hacerles vivir experiencias inolvidables.

10.4.4 Innovación

Trabajamos permanentemente en desarrollar y potenciar en la organización y en nuestro talento humano la capacidad de crear y poner en práctica nuevas ideas, para asegurar la alineación con un mundo en constante cambio y transformación.

10.4.5 Solidaridad

Mantenemos la determinación firme y perseverante de comprometernos por el bien común, con criterios de responsabilidad social.

10.5 GESTION TECNOLOGICA COMFAGUAJIRA

10.5.1 OBJETIVO

Garantizar de manera eficaz la planeación, análisis e incorporación de soluciones tecnológicas e informáticas que contribuyan a determinar, proporcionar y mantener los servicios de tecnologías de información, necesarios para el logro de los objetivos estratégicos de Comfaguajira.

10.5.2 ALCANCE

Aplica para toda los servicios de Tecnologías de la información de Comfaguajira en sus diferentes sedes y áreas. Incluye las actividades del plan estratégico de tecnologías de información, entrenamiento y asesorías en tecnología, mantenimiento de activos de T.I y administración del sistema de información corporativa.

10.5.3 PROCESOS ASOCIADOS

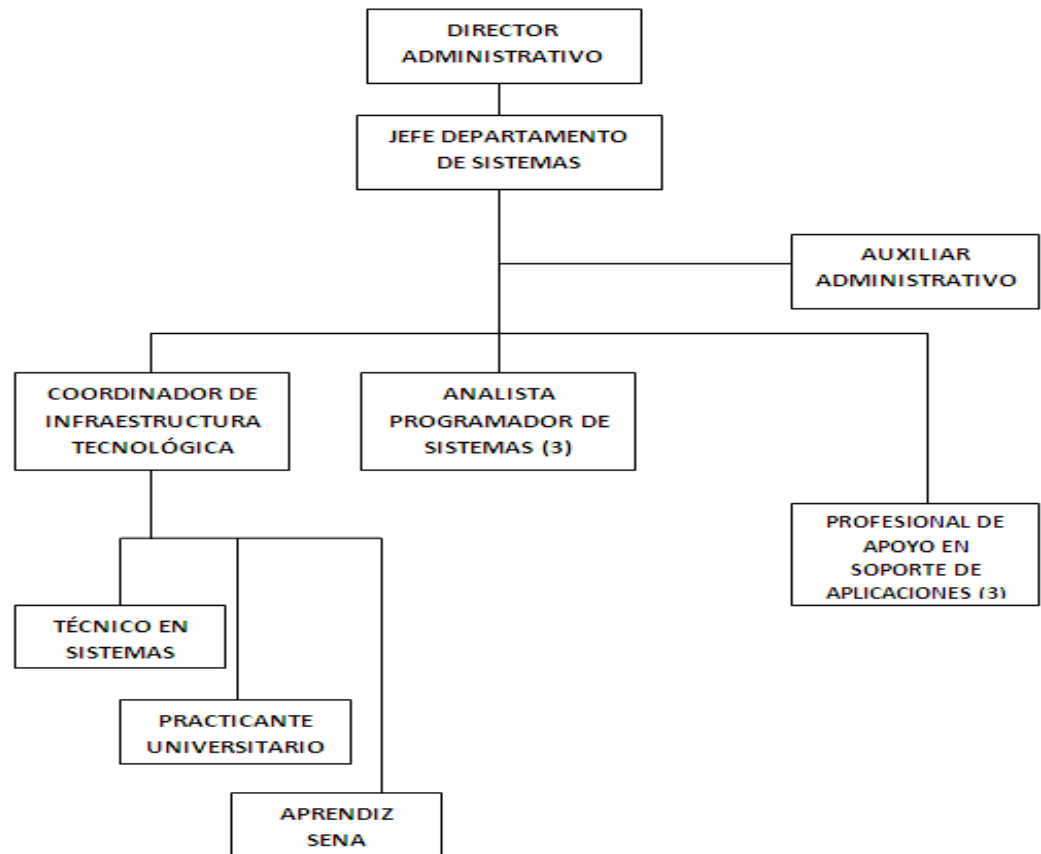
10.5.3.1 LOGISTICA

Apoyo en la adquisición de paquetes tecnológicos y gestión de activos

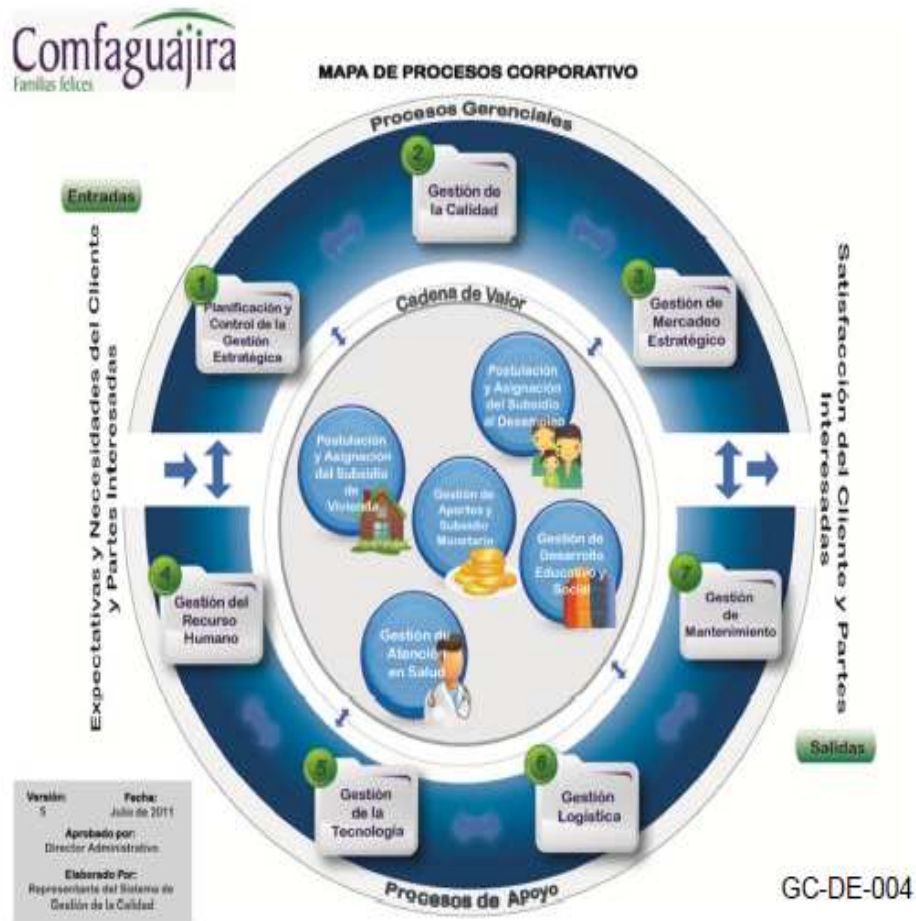
10.5.3.2 PLANEACION

Plan estratégico corporativo y aprobación del plan tecnológico y de mantenimiento tecnológico

10.6 ORGANIGRAMA DEL DEPARTAMENTO DE SISTEMAS DE COMFAGUAJIRA



10.7 MAPA DE PROCESO CORPORATIVO DE COMFAGUAJIRA



10.8 ACTIVOS DE TI

CATEGORIAS	ACTIVOS
Activos de Información	Base de datos Registros de voz Archivos de imágenes Documentación del Sistema Manuales de usuario Material de entrenamiento Procedimientos operacionales o de soporte Planes de continuidad
Documentos físicos	Contratos Guías Documentación de la compañía Licencias de software
Activos de software	Software de aplicación Software del sistemas Herramientas de desarrollo y utilidades Medios magnéticos
Servicios	Servicios de comunicación Servicios de procesamiento Servicios de correo electrónico Iluminación Energía Ventilación
Otros equipos	Planta de energía Unidades de aire acondicionado Equipos de comunicación Computadoras Servidores Activos fijos Infraestructura de red y cableado Medios de almacenamiento físico Estaciones de trabajo Sistema de respaldo (UPS)
Personas	Personal interno de TI

10.12 METODOLOGIA

Para el logro de los objetivos se aplicara la siguiente metodología:

- Recolectar toda la información referente a los procesos auditados
- Realizar una entrevista junto al jefe de sistemas y algunos funcionarios de la caja.
- Aplicar técnicas de inspección, verificación y revisión de los controles que afecten a los procesos, objetos del estudio, en la caja.
- Realizar una lista de riesgos y una lista de controles implantados para minimizar los riesgos.
- Desarrollar las matrices correspondientes las cuales diagnosticaran el análisis de los riesgos.

10.13 ACTIVIDADES

10.13.1 Técnicas de trabajo

- Recolectar información con respecto al área auditada.
- Análisis de la información recolectada.
- Cruzamiento de las informaciones anteriores.
- Enfoque hacia los procesos tecnológicos de la caja.

10.14 INVERSION

DESCRIPCION	COSTO
Papelería	330.000
Impresiones	250.000
Alquiler equipo PC	450.000
Servicio de Internet	360.000
Fotocopias	150.000
Transporte	700.000
Horas utilizadas hombre utilizadas en el proyecto	\$ 8.000.000

**10.4 AUTODIAGNOSTICO MEDIANTE COSO DE LOS RIESGOS DE LA GESTION
TECNOLOGICA COMFAGUAJRA**

10.15.1 ARQUITECTURA DE HARDWARE Y SOFTWARE						2,07
S N NA						
1	¿La entidad dispone de planes de desarrollo de sistemas, cambio en hardware y software para el siguiente año?	x			Se debe realizar la priorización de los proyectos y sus presupuestos	3,00
2	¿Existe control del Inventario de Hardware?	x			Existe dificultades en su actualización	2,00
3	¿La Depreciación del hardware se realiza de acuerdo con las exigencias legales?	x				1,00
4	¿El valor contable de los equipos no excede el valor de realización?			x		
5	¿Los equipos se encuentran asignados por escrito mediante un acta entrega recepción a las personas que los utilizan?	x				1,00
6	¿La entidad dispone de Políticas escritas sobre el licenciamiento de software?	x			Se encuentran en revisión	2,00
7	¿Se han establecido restricciones para la utilización de programas no autorizados por la entidad?	x			Falta más sensibilización y controles	2,00
8	¿Existen acuerdos con los proveedores de equipos (Hardware) para el reemplazo inmediato de componentes en caso de fallas?	x			El tiempo de respuesta de algunos proveedores no es oportuno	3,50

10.15.2 PLAN ESTRATÉGICO DE SISTEMAS						1,70
9	¿Se elabora un presupuesto para el área de sistemas?	x				1,00
10	¿Se ejecutan procedimientos de evaluación a los integrantes del área de sistemas?	x			Alineación del feedback y el Plan Operativo Anual	2,00
11	¿Están adecuadamente segregadas las tareas entre el personal del área de sistemas y de las áreas usuarias?	x			Se debe establecer responsabilidades en el manejo de la información por parte de los usuarios	2,50
12	¿Se elaboran actas de las reuniones del área de sistemas?	x				1,00
13	¿Existen políticas de entrenamiento y de desarrollo de personal para el área de sistemas?	x			Mejorar el entrenamiento Técnico del área	2,00
10.15.3 DESARROLLO DE SISTEMAS DE INFORMACIÓN						3,00
14	¿Existe una guía escrita de procedimientos diarios a realizarse en la operación diaria del computador principal?		x			4,00
15	¿Están asignadas las tareas y responsabilidades específicas a cada persona del área de operaciones?	x			No está especificado por persona, esta por cargo	3,00
16	¿Existen procedimientos de recuperación de información y son probados periódicamente?	x			No han sido probados	3,00

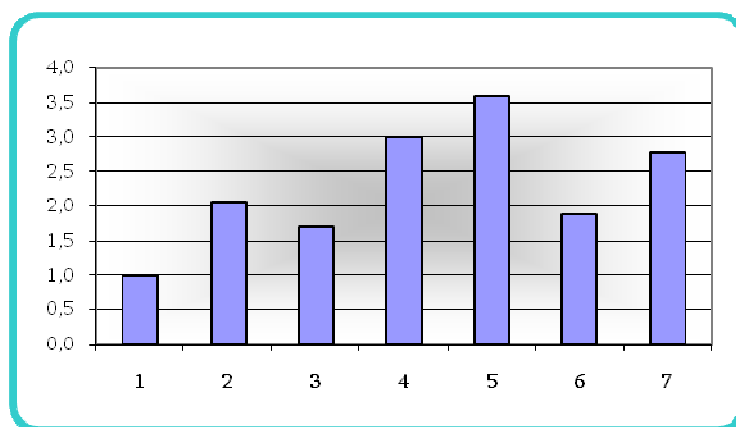
17	¿Se han definido procedimientos para la creación de respaldos de la información?	x			Se deben actualizar	2,00
10.15.4 RESPALDO DE LA INFORMACIÓN						3,60
18	¿Se han definido procedimientos de recuperación de respaldos?	x			Se deben actualizar	3,00
19	¿Existe un plan de recuperación en caso de desastres?		x			4,00
20	¿Existen procedimientos para el mantenimiento de UPS, prueba y activación?		x			4,00
21	¿Se han definido estrategias para la protección de los respaldos?		x			4,00
22	¿Se guarda periódicamente un respaldo de la información y los programas fuera de la entidad?	x			Los respaldos no se almacenan fuera de la entidad.	3,00
10.15.5 SEGURIDAD FÍSICA DE LA INFORMACIÓN						1,88
23	¿Se restringe el acceso a las instalaciones de la CAJA (Edificio, sala de máquinas)?	x			Mejorar la política de acceso	1,50
24	¿Se encuentra controlado el acceso al hardware las 24 horas?	x			Mejorar los puntos de red de (Gabinetes comunicación)	2,00
25	¿Se restringe y controla el acceso a la sala del servidor principal?	x				1,00

26	¿Se impide y controla el acceso a las computadoras?	x			Mejorar las políticas y configuración de los usuarios de Red	3,00
27	¿Se ha elaborado y actualizado una lista de personal autorizado y con accesos a la sala de máquinas?	x				1,00
28	¿Existen detectores de humo, fuego y equipo de seguridad, y se prueban periódicamente?		x			4,00
29	¿El ambiente de trabajo está protegido de la humedad y el polvo?	x			Realizar seguimiento de control de humedad	1,50
30	¿Se restringe el acceso a Internet?	x				1,00
10.15.6 SEGURIDAD LÓGICA DE LA INFORMACIÓN						2,78
31	¿Se han establecido políticas generales de seguridad y políticas de seguridad de los datos y la información?	x			Está en proceso de actualización	2,00
32	¿Estándares para la configuración de parámetros de seguridad en los sistemas de información (usuarios, grupos, validaciones)?	x			Revisar los permisos de los grupos según el perfil de cargo	2,00
33	¿Existen estándares de seguridad en el procesamiento de datos?		x			3,00
34	¿Se ha designado al responsable por el cumplimiento de las políticas y procedimientos de seguridad de la	x				2,00

	información?					
35	¿Existe un software de seguridad?		x		Solo de acceso a internet	3,00
36	¿Se deja evidencia o registro de accesos indebidos?		x			3,00
37	¿Se actualizan los accesos a los sistemas de información en el caso de retiro de empleados?	x			No es oportuno la información	3,00
38	¿Se usan claves e identificadores personales para restringir el acceso a los comandos del sistema operativo?	x			Se debe mejorar la configuración de los usuarios de red	3,00
39	¿Se usan claves e identificadores personales para restringir el acceso a los programas?	x			Se debe mejorar la seguridad de las claves	2,00
40	¿Se cambian las claves periódicamente?		x		Falta de cultura en el manejo de las claves	3,00
41	¿Existe confidencialidad de las claves de acceso?		x		Falta de cultura en el manejo de las claves	4,00
42	¿Hay restricciones para evitar la copia de programas?		x			4,00
43	¿Son las modificaciones a los programas realizados por las personas calificadas?			x		-
44	¿Son los pedidos de modificación a los programas documentados por los usuarios y el administrador del sistema?			x		-

45	¿Se han establecido políticas para el uso de las computadoras personales?		x			3,00
46	¿Existen procedimientos para el respaldo de datos en computadores personales?		x		Depende de la política de uso de computadores personales	3,00
47	¿Se han definido estándares para el uso de software antivirus en computadores personales y servidores?	x				2,00
48	¿Existen, procedimientos a seguir en caso de aparición de virus en los computadores personales?	x				2,50

1	NORMATIVIDAD INTERNA	1,0	1	Riesgo Bajo
2	ARQUITECTURA DE HARDWARE Y SOFTWARE	2,1	2	Riesgo Moderado
3	PLAN ESTRATÉGICO DE SISTEMAS	1,7	3	Riesgo Bajo
4	DESARROLLO DE SISTEMAS DE INFORMACIÓN	3,0	4	En Riesgo
5	RESPALDO DE LA INFORMACIÓN	3,6	5	En Riesgo
6	SEGURIDAD FÍSICA DE LA INFORMACIÓN	1,9	6	Riesgo Moderado
7	SEGURIDAD LÓGICA DE LA INFORMACIÓN	2,8	7	En Riesgo



10.16 RESULTADO DEL DIAGNOSTICO INICIAL DE RIESGOS

Antes de iniciar a identificar los riesgos de la gestión tecnológica de la Caja de Compensación Familiar de la Guajira “COMFAGUAJIRA”, se elaboró una lista de chequeo según el marco de referencia COSO, con el fin de elaborar un diagnóstico inicial de los riesgos que afronta la gestión tecnológica según criterios como NORMATIVA INTERNA, ARQUITECTURA DE HARDWARE Y SOFTWARE, PLAN ESTRATEGICO, DESARROLLO DE SISTEMAS DE INFORMACION, RESPALDO DE INFORMACION, SEGURIDAD FISICA Y SEGURIDAD LOGICA, en la cual se evaluó cada una de las preguntas en un rango de 1 a 4 en la que 1 significaba menor riesgo y 4 mayor riesgo, la cual fue resuelta en la segunda

entrevista que se realizó con la Jefe del departamento de sistemas de la caja la ingeniera Marisol Henríquez Vázquez.

Este diagnóstico inicial permitió identificar los puntos clave que deben ser tenidos en cuenta al momento de iniciar el levantamiento de los riesgos para la elaboración de la matriz de riesgo que dará como resultado este proyecto.

Se logró identificar inicialmente que la NORMATIVA INTERNA y PLAN ESTRATEGICO se encuentra en riesgo bajo, ya que se han tomado medidas suficientes para reducir los riesgos ocasionados por estos riesgos.

Se encuentran en riesgo moderado ARQUITECTURA DE HARDWARE Y SOFTWARE y LA SEGURIDAD FISICA, ya que existen aún tareas por evaluar y mejorar para mitigar correctamente los riesgos.

10.17 VALORACION DE LOS RIESGOS

10.17.1 MATRIZ DE CRITERIOS PARA CALIFICAR EL IMPACTO		
NIVELES PARA CALIFICA IMPACTO	IMPACTO CUANTITATIVO	IMPACTO CUALITATIVO
SUPERIOR	Impacto que afecte el margen financiero en un 10% o más del valor proyectado. Perdida de participación de mercado superior al 1%	<p>Interrupción de las operaciones de la entidad por más de 2 días.</p> <p>Sanciones económicas por incumplimiento de las normas establecida por los ente reguladores.</p> <p>Impacto que genera una imagen negativa de la entidad en el mercado</p> <p>Perdida de información crítica de la entidad o de terceros que no se pueda recuperar</p>
MAYOR	<p>impacto que afecte el margen financiero entre un 6% y 10% del valor proyectado</p> <p>perdida de participación de mercado superior al 0,8%</p>	<p>Interrupción de las operaciones de la compañía por 2 días</p> <p>Observaciones por incumplimiento de las normas establecidas por los entes reguladores que generen un plan de acción a corto plazo</p> <p>Impacto que afecte la imagen de la entidad en el mercado.</p> <p>Perdida de información crítica de entidad o de terceros que no se pueda recuperar fácilmente</p>
IMPORTANTE	<p>Impacto que afecte el margen financiero entre un 3% y 6% del valor proyectado</p> <p>Perdida de participación de</p>	<p>Interrupción de las operaciones de la compañía por 1 día</p> <p>Reclamaciones de clientes y/o proveedores que requieren de</p>

	mercado superior al 0,5%	<p>un plan de acción a corto plazo y podrían afectar la continuidad de la relación</p> <p>Inoportunidad de la información ocasionando retrasos en las labores de las áreas y/o en la respuesta a los entes reguladores</p> <p>Reproceso de actividades y aumento de la carga operativa</p>
MENOR	<p>Impacto que afecte el margen financiero entre un 1% y 3% del valor proyectado</p> <p>Perdida de participación de mercado superior al 0,2%</p>	<p>Interrupción de las operaciones de la compañía por algunas horas</p> <p>Existe reclamaciones por parte de los clientes y/o proveedores pero no se afecta la continuidad de la relación</p> <p>No afecta la oportunidad de la información de manera significativa, no altera el funcionamiento de las áreas receptoras de información</p>
INFERIOR	<p>Impacto que afecte el margen financiero en menos de un 1% del valor proyectado</p> <p>No hay pérdida de participación de mercado</p>	<p>No hay interrupción de las operaciones de la entidad</p> <p>No genera sanciones económicas y/o administrativas</p> <p>No afecta las relaciones con los clientes y/o proveedores</p> <p>No afecta la oportunidad de la información</p>

10.17.2 MATRIZ DE CRITERIOS PARA CALIFICAR LA PROBABILIDAD	
NIVELES PARA CALIFICA PROBABILIDAD DE OCURRENCIA	DESCRIPCION
MUY ALTA	Se espera la ocurrencia del evento en el 80% de los casos Casi con certeza se espera la ocurrencia del evento Nos ocurre con cierta periodicidad (1 vez cada mes)
ALTA	El evento ocurría entre el 50 y el 80% de los casos Significativa probabilidad de ocurrencia Se presenta con alguna frecuencia (1 vez cada trimestre)
MODERADO	El evento puede ocurrir entre 20 y 50% de los casos Mediana probabilidad de ocurrencia Se presenta por lo menos una vez cada año
BAJA	El evento puede ocurrir entre 5 y 20% de los casos Baja probabilidad de ocurrencia Se ha presentado alguna vez en la entidad o en el sector
MUY BAJA	El evento puede ocurrir en menos del 5% de los casos Muy baja probabilidad de ocurrencia Nunca ha ocurrido

CONCLUSION

Comfaguajira es una organización en aras de crecer y expandir sus servicios a muchas más personas para cumplir con su lema, hacer ' familias felices', para esto se hace que se enfrente a diversos riesgos en el área tecnológica, la cual está sirviendo de apoyo para la obtención de todas las metas estratégicas que esta se ha planteado.

Después de la elaboración del análisis de riesgos a Comfaguajira se logro encontrar que existe muy poca documentación y procedimientos estructurados que ayuden a apoyar de forma oportuna las necesidades tecnológicas de la organización, que además ocasionan que el proceso de la gestión tecnológico sea más un apague de fuegos y no un proceso planeado, organizado y controlado que permita que se genere mejora continua de los procesos tecnológicos que afecta el adecuado desempeño de la organización.

Los riesgos no están siendo adecuadamente controlados, los controles que actualmente existen en la organización no están documentados y mucho menos controlados de manera adecuada con el fin de evaluar su efectividad.

Existen riesgos importantes que no tienen ningún control definido para este y en algunos casos, no se consideraban como riesgos que podrían afectar de forma importante o catastrófica a la organización.

A pesar de que la organización ha empezado a darse cuenta de la importancia de controlar adecuadamente los riesgos que afronta, no posee ninguna metodología para hacerlo y mucho menos el presupuesto necesario para iniciar el proceso de encarar adecuadamente los riesgos que afronta.

En el departamento de sistemas no existe un adecuado ambiente de control, ya que cada funcionario es responsable de sus funciones y no hay un adecuado control de todo el proceso tecnológico como un conjunto desde un ángulo imparcial que conozca la infraestructura tecnológica de la caja.

La organización no posee un auditor de sistemas encargado de controlar el adecuado manejo de los riesgos tecnológicos de la organización, en la caja solo se auditan los sistemas contable pero no la infraestructura tecnológica en la que se apoyan todos los procesos de la empresa y su inadecuado manejo afecta considerablemente los recursos económicos de la organización.

La caja vio la necesidad del análisis de riesgos tecnológicos por la obligatoriedad de la implementación de la circular 023 de 2010 de la superintendencia del subsidio familiar, y a partir de este a logrado detectar las grandes debilidades y amenazas que atacarían de forma catastrófica la continuidad y recursos económico de la caja.

Se evidencio que existe gran interés por sacar adelante la gestión de los riesgos de la gestión tecnológica por parte de la dirección de la caja, ya que se percataron de las grandes falencias encontradas, por lo cual desean atacar de forma oportuna las amenazas y vulnerabilidades que atacan a la caja en estos momentos.

La caja se encuentra actualmente en un proceso de mejoramiento sobre todo en la gestión tecnológica, comenzando con la creación y puesta en marcha de su planeación estratégica de TI y de la implantación de las policitas de seguridad, entre otras actividades, todas enfocadas con el fin de brindarle mayor satisfacción a sus usuarios y proporcionarle efectivamente el apoyo a las metas estratégicas de la caja.

RECOMENDACIONES

A raíz del análisis de riesgos realizado a la caja de compensación de la guajira COMFAGUAJIRA, se realizaron las siguientes recomendaciones:

- Implementar controles preventivos, correctivos y detectivos a cada uno de los riesgos, iniciando primero con los más críticos o catastrófico, que se hayan identificado con el fin de disminuir en alto grado el impacto y la probabilidad de ocurrencia, además se deben implementar no solo controles manuales sino controles automatizados que generen bitácoras, indicadores y evidencias para posteriores tomas de decisiones.
- Dar prioridad a los riesgos de mayor riesgo, con el fin de implementar controles que puedan disminuir considerablemente su impacto y probabilidad y luego continuar con los otros riesgos menores.
- Se deben evaluar los análisis costo beneficio de los controles para que estos no se conviertan en generadores de nuevos riesgos no controlados o desconocidos que puedan afectar la organización y además que no se realice una inversión que no se justifique, ya que el control es más costoso que el impacto económico que genere el riesgo.
- Se debe realizar un análisis de riesgo anualmente en vista que las condiciones ambientales, económicas, tecnológicas y legales cambian con mucha frecuencia y sobre todo cambia las necesidades de la organización y las herramientas que TI utiliza para apoyarlas.
- Es necesario que sean evaluada la eficiencia y oportunidad de los controles implementados a los diversos riesgos, con el fin de saber si están siendo eficientes en la tarea de reducir el impacto y probabilidad de los riesgo, de lo contrario tomar

medidas sobre mejorarlo o cambiarlo oportunamente, antes de que se presente algún incidente catastrófico no esperado.

- Es de suma importancia que en el análisis de riesgo intervengan diversas personas que trabajen o afecten la gestión tecnológica de la caja, con el fin de tener diversos puntos de vistas de los distintos riesgos que esta se enfrenta, además se requiere que exista un gran compromiso para que este proceso sea un éxito, iniciando con la dirección, con el fin de que sea un proceso institucional y que todos lo que intervengan estén comprometidos en el proceso.
- Es necesario que el análisis no se base en la experiencia de otras cajas, sino que se base en la propia ya que a pesar que tienen el mismo core, no manejan los procesos de la misma forma, no poseen la misma infraestructura, además se encuentran en un ambiente distinto y sobre todo en ellas trabajan personal totalmente variado, por lo cual no se debe tener en cuenta la experiencia de las demás cajas.
- Es necesario que el proceso tecnológico de la caja posea un auditor de sistemas, ya sea interno o externo, el cual les ayude con el proceso de análisis de riesgos de una forma efectiva y proporcione la información necesaria para la toma de decisiones.
- Que evalúen las diversas posibilidades de transferir a terceros los riesgos por medio de seguros, outsourcing, leasing entre otras, para enfrentar los diversos riesgos.
- El departamento de sistemas de la organización sea capacitado sobre las diversas metodológicas de análisis de riesgos que les permitan continuar el proceso y no se queden con el análisis inicialmente elaborado, con el fin de que puedan analizar los diversos riesgos que aparecerán con el cambio del negocio, ambiente y economía.
- Implementar en el departamento de sistemas un adecuado ambiente de control para que pueda implementar todos los mecanismos necesarios para afrontar los

riesgos que podrían causar un impacto catastrófico en la infraestructura, imagen o economía de la organización.

- Cada nuevo proyecto que emprenda el departamento de sistemas de la caja debe incluir un análisis de los riesgos que estos puedan ocasionar y afecten el correcto desarrollo del proyecto.

BIBLIOGRAFIA

Circular 023, Superintendencia del subsidio Familiar

<http://www.comfama.com/contenidos/servicios/Subsidio/Marco%20legal/marcolegal.asp>

<http://www.youblisher.com/p/52860-COSO/>

<http://www.overti.es/procesos-itsm/cobit.aspx>

<http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf>

<http://www.comfaguajira.com/>

<http://www.comfaguajira.com/articulo.aspx?idc=51>

[http://www.comfaguajira.com/media/archivos/Codigo de etica.pdf](http://www.comfaguajira.com/media/archivos/Codigo_de_etica.pdf)

<http://www.actualicese.com/normatividad/2010/11/30/circular-externa-0023-de-30-11-2010/>

http://www.ssf.gov.co/wps/wcm/connect/wcm_ssf/ssf/normatividad+del+subsidio+familiar/circulares+2010

CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO DE TESIS Y TRABAJOS DE GRADO

Barranquilla, Enero 27 de 2012

Marque con una X
Tesis ☐ Trabajo de Grado ☐

Yo **ROSA INES ESTUPIÑAN MEJIA**, identificada con C.C. No. **40.941.801**, actuando en nombre propio y como autor de la tesis y/o trabajo de grado titulado **DISEÑO DEL ANALISIS DE RIESGO DEL PROCESO TECNOLÓGICO DE LA CAJA DE COMPENSACIÓN FAMILIAR DE LA GUAJIRA "COMFAGUAJIRA", PARA LA APLICACIÓN DEL SISTEMA DE CONTROL INTERNO SUBSIDIO FAMILIAR SCISF, SEGÚN CIRCULAR 0023 DEL 30 DE NOVIEMBRE DE 2010, DE LA SUPERINTENDENCIA DE SUBSIDIO FAMILIAR DURANTE EL SEGUNDO SEMESTRE DEL 2011** presentado y aprobado en el año **2012** como requisito para optar al título de Especialista en **AUDITORÍA DE SISTEMAS DE INFORMACIÓN**; hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la CORPORACIÓN UNIVERSITARIA DE LA COSTA, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Corporación Universitaria de la Costa, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de información del país y del exterior, con las cuales tenga convenio la institución y Permita

la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los **27** días del mes de **Enero** de Dos Mil **Doce** 2012

EL AUTOR - ESTUDIANTE. _____

FIRMA

CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO DE TESIS Y TRABAJOS DE GRADO

Barranquilla, Enero 27 de 2012

Marque con una X
Tesis ☐ Trabajo de Grado ☐

Yo **MIRLEDIS ELENA MARTINEZ LEAL**, identificado con C.C. No. **1.118.800.810**, actuando en nombre propio y como autor de la tesis y/o trabajo de grado titulado **DISEÑO DEL ANALISIS DE RIESGO DEL PROCESO TECNOLÓGICO DE LA CAJA DE COMPENSACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA”, PARA LA APLICACIÓN DEL SISTEMA DE CONTROL INTERNO SUBSIDIO FAMILIAR SCISF, SEGÚN CIRCULAR 0023 DEL 30 DE NOVIEMBRE DE 2010, DE LA SUPERINTENDENCIA DE SUBSIDIO FAMILIAR DURANTE EL SEGUNDO SEMESTRE DEL 2011 DURANTE EL SEGUNDO SEMESTRE DEL 2011** presentado y aprobado en el año **2012** como requisito para optar al título de Especialista en **AUDITORÍA DE SISTEMAS DE INFORMACIÓN**; hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la CORPORACIÓN UNIVERSITARIA DE LA COSTA, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Corporación Universitaria de la Costa, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de

información del país y del exterior, con las cuales tenga convenio la institución y Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los 27 días del mes de Enero de Dos Mil Doce 2012

EL AUTOR - ESTUDIANTE._____

FIRMA

FORMULARIO DE LA DESCRIPCIÓN DE LA TESIS O DEL TRABAJO DE GRADO

TÍTULO COMPLETO DE LA TESIS O TRABAJO DE GRADO: “DISEÑO DEL ANALISIS DE RIESGO DEL PROCESO TECNOLÓGICO DE LA CAJA DE COMPENSACIÓN FAMILIAR DE LA GUAJIRA “COMFAGUAJIRA”, PARA LA APLICACIÓN DEL SISTEMA DE CONTROL INTERNO SUBSIDIO FAMILIAR SCISF, SEGÚN CIRCULAR 0023 DEL 30 DE NOVIEMBRE DE 2010, DE LA SUPERINTENDENCIA DE SUBSIDIO FAMILIAR”

SUBTÍTULO, SI LO TIENE:

AUTOR AUTORES

Apellidos Completos	Nombres Completos
Estupiñan Mejía	Rosa Inés
Martínez Leal	Mirledis Helena

DIRECTOR (ES)

Apellidos Completos	Nombres Completos
Montaño Ardila	Víctor Manuel

JURADO (S)

Apellidos Completos	Nombres Completos
Ramos	Fabián
Neira	Harold

ASESOR (ES) O CODIRECTOR

Apellidos Completos	Nombres Completos

TRABAJO PARA OPTAR AL TÍTULO DE: Especialista en Auditoría de Sistemas de Información

FACULTAD: Ciencias Económicas

PROGRAMA: Pregrado ____ Especialización X

NOMBRE DEL PROGRAMA: Especialización en Auditoría de Sistemas de Información

CIUDAD: Barranquilla **AÑO DE PRESENTACIÓN DEL TRABAJO DE GRADO:** 2012

NÚMERO DE PÁGINAS 157

TIPO DE ILUSTRACIONES:



Ilustraciones



Láminas



Retratos



Tablas, gráficos y diagramas



Planos



Mapas



Fotografías

MATERIAL ANEXO (Vídeo, audio, multimedia o producción electrónica):

Duración del audiovisual: _____ minutos.

Número de casetes de vídeo: _____ Formato: VHS ____ Beta Max ____ ¾ ____ Beta Cam

____ Mini DV ____ DV Cam ____ DVC Pro ____ Vídeo 8 ____ Hi 8 ____

Otro. Cuál? _____

Sistema: Americano NTSC _____ Europeo PAL _____ SECAM _____

Número de casetes de audio: _____

Número de archivos dentro del DVD (En caso de incluirse un DVD diferente al trabajo de grado):

PREMIO O DISTINCIÓN *(En caso de ser LAUREADAS o tener una mención especial):*

DESCRIPTORES O PALABRAS CLAVES EN ESPAÑOL E INGLÉS:

ESPAÑOL

Análisis de Riesgo _____

INGLÉS

Risk Analysis _____

Ambiente de Control _____

Control Environment _____

RESUMEN DEL CONTENIDO EN ESPAÑOL E INGLÉS (Máximo 250

palabras-1530 caracteres):

Este proyecto fue realizado con el fin de ofrecerle a COMFAGUAJIRA, las herramientas necesarias para iniciar la implementación de la circular 023 de 2010 de la Superintendencia de Subsidio Familiar, la cual obliga a las cajas de compensación de Colombia a implementar un sistema de control interno en todos sus procesos entre los cuales esta la gestión tecnológica, con el fin de que estas implementen los siguientes conceptos:

AUTOGESTION: Capacidad de interpretar, coordinar, ejecutar y evaluar de manera efectiva, eficiente y eficaz su funcionamiento.

AUTOCONTROL: Capacidad de cada uno de los funcionarios para evaluar, mejorar y controlar su trabajo.

AUTOREGULACION: Capacidad de la entidad de aplicar métodos, normas y procedimientos que permitan el desarrollo, implementación y mejoramiento del Sistema de Control Interno.

SUMMARY

This project was undertaken to COMFAGUAJIRA offer the tools necessary to begin implementation of Circular 023 of 2010 of the Superintendency of Family Subsidy, which requires the compensation of Colombia to implement a system of internal control all the processes including the management of technology, so that these implement the following:

SELF MANAGEMENT: The ability to interpret, coordinate, implement and evaluate effective, efficient and effective functioning.

SELF CONTROL: The ability of each staff to evaluate, improve and control their work.

SELF REGULATION: The ability of the entity to apply methods, standards and procedures for developing, implementing and improving the System of Internal Control.